Sonera CA

Varmennuskäytäntö

Voimassa 2.12.2008 lähtien
Versio 2.5

Varmenteet yrityskäyttöön

Sonera Class 1 -varmenne
Sonera Class 2 -varmenne
Sonera Mobiilivarmenne

Tämä suomenkielinen versio on epävirallinen käännös englanninkielisestä dokumentista ”Sonera CA Certification Practice Statement” joka on alkuperäinen ja virallinen varmennuskäytäntö.

TeliaSonera Finland Oyj

Varmennuskäytännön TeliaSonera Finland CPS-1 versionhallinta

Versionumero	Dokumentin nimi	Päivämäärä	Kuvaus
V 1.0	Sonera Certificate Authority, CPS – Certification Practice Statement	1.1.2001	Ensimmäinen Sonera CA varmennuskäytäntö
V 1.1	Ks. yllä	1.3.2001	Tarkennuksia
V. 2.0	Sonera CA, Varmennuskäytäntö	22.9.2003	Rakenteen muutos
V. 2.1	Ks. yllä	22.1.2004	Tarkennuksia
V. 2.2	Ks. yllä	30.5.2005	Tarkennuksia
V. 2.3	Ks. yllä	15.6.2007	Tarkennuksia ja pieniä muutoksia
V. 2.4	Ks. yllä	2.10.2007	Ali-CA määritykset lisätty
V. 2.5	Ks. yllä	13.11.2008	Muutoksia luvuissa 3.2.5.1, 4.4.3.2, 5.2.2, 6.1.1 ja 6.1.4

Kaikki julkaistut versiot ovat saatavissa osoitteesta:
http://support.partnergate.sonera.com/.

Sisällysluettelo

TeliaSonera Finland Oyj

Määritelmiä

Ali-CA: *CA, jonka varmenteiden allekirjoitusavaimen on allekirjoittanut toinen CA. Ali-CA:n toiminta määräytyy kyseisen toisen CA:n mukaan.*

Aktivointitieto*: Tunnusluku (esim. PIN-koodi), jolla Varmenteen haltija aktivoi yksityisen avaimensa. Tunnusluku on annettava erikseen joka kerta kun avainta käytetään.*

Allekirjoituksen luomisväline, Signature Creation Device (SCD): *Varmenne-SIM -kortti, USB-avain, PKCS#12-tiedosto tai toimikortti, joka sisältää Varmenteen haltijan yksityisen avaimen.*

Asiakasorganisaatio*: TeliaSonera Finland Oyj:n (jäljempänä "Sonera") yritysasiakas, joka käyttää Soneran varmennepalveluita.*

Avainpari: *Varmenteen haltijan käytössä oleva yksityinen avain ja siihen liittyvä julkinen avain muodostavat avainparin.*

Issuer: *Varmenteen kenttä, jossa määritellään varmenteen allekirjoittanut Varmentaja.*

Julkinen avain, Public key: *Varmenteen haltijalle kuuluvan asymmetrisen avainparin se osa, joka on Luottavien osapuolten käytössä.*

Julkisen avaimen infrastruktuuri, Public Key Infrastructure (PKI)*: Infrastruktuuri, joka koostuu ohjelmistosta, laitteistosta, henkilöistä, politiikoista ja menettelytavoista, jotka hyödyntävät julkisen avaimen salaustekniikkaa ja joiden avulla voidaan luoda, hallinnoida, säilyttää, jakaa ja peruuttaa varmenteita [PKIX Roadmap].*

Luottava osapuoli*: Osapuoli, joka luottaa varmenteessa oleviin tietoihin tehdessään päätöksiä [ISO/IEC 9594-8; ITU-T X.509].*

Rekisteröijä, Registration Authority, (RA): *Osapuoli, joka on vastuussa Varmenteen haltijan tunnistamisesta, mutta joka ei allekirjoita tai myönnä varmenteita (ts., RA hoitaa tiettyjä toimintoja Varmentajan puolesta) [RFC 2527].*

Rekisteröintivastaava: *Henkilö, joka suorittaa Rekisteröijälle kuuluvia tehtäviä vastuullaan mm. Varmenteiden luonnin ja jakelun hyväksyntä.*

Salaustekninen laite: *Varmentajan käytössä oleva ohjelmistoa ja elektroniikkaa sisältävä laite, joka toteuttaa salausteknisiä algoritmeja ja jota käytetään Varmentajan salausavainten luomisen, tallennuksen ja käytön tietoturvan takaamiseksi.*

Salaustekninen väline: *Varmenteen haltijan käytössä oleva väline, jolle hänen yksityinen avaimensa on tallennettu ja joka toteuttaa salausteknisiä algoritmeja. Sonera PKI:ssä salaustekninen väline on toimikortti tai USB avain, joka toimii allekirjoituksen luomisvälineenä.*

SAP-tila: *Matkapuhelinliittymä on SAP-tilassa silloin kun se on suljettu asiakkaan pyynnöstä siten, että se voidaan vielä palauttaa käyttöön. SAP-tila estää matkapuhelinlittymästä kaiken tulevan ja lähtevän liikenteen.*

Sonera: *Termi tarkoittaa tässä dokumentissa TeliaSonera Finland Oyj:tä.*

Sonera Class2 CA: *Tämä CA voi myöntää Ali-CA varmenteita. Ali-CA:n avain tallennetaan salaustekniseen laitteeseen.*

Sonera Class 1 -varmenne: *Varmenne, joka myönnetään luonnolliselle henkilölle. Varmenne ja siihen liittyvä yksityinen avain on tallennettu salaustekniselle välineelle. (Käytetään jatkossa lyhennettä "Class 1".)*

Sonera Class 2 -varmenne: *Varmenne, joka myönnetään luonnolliselle henkilölle tai Laitteelle. Varmenne ja siihen liittyvä yksityinen avain on tallennettu ohjelmistoon. (Käytetään jatkossa lyhennettä "Class 2".)*

Sonera Mobiilivarmenne: *Varmenne, joka myönnetään luonnolliselle henkilölle. Varmenteeseen liittyvä yksityinen avain on tallennettu Varmenne-SIM -kortille. (Käytetään jatkossa lyhennettä "Mobiilivarmenne".)*

Sonera PKI: *Infrastruktuuri, joka koostuu ohjelmistosta, laitteistosta, käytännöistä, menettelytavoista ja politiikoista, joita hallinnoi Sonera CA. Sonera PKI:n avulla pystytään tarjoamaan julkisen avaimen järjestelmää ja varmennusmenettelyjä käyttäviä turvapalveluita.*

Sulkulista, Certificate Revocation List, (CRL): *Lista, joka sisältää tietyn varmentajan myöntämien peruutettujen varmenteiden sarjanumerot sekä muuta peruuttamiseen liittyvää tietoa.*

Sulkulistapalvelu: *Palvelu, josta Luottavat osapuolet voivat tarkistaa onko varmenne peruutettu (esim. hakemisto).*

Sulkupalvelu: *Osapuoli, joka hoitaa varmenteiden peruuttamispyyntöjen vastaanottamisen ja lähettää oikeutetut peruuttamispyynnöt edelleen Varmentajalle.*

Sähköinen allekirjoitus: *Sähköisessä muodossa oleva tieto, joka on liitetty tai joka loogisesti liittyy muuhun sähköiseen tietoon ja jota käytetään allekirjoittajan henkilöllisyyden todentamisen välineenä [SAK Laki].*

Tietovarasto: *Järjestelmä, johon Varmentaja on tallentanut varmennustoimintaansa liittyvät julkiset dokumentit ja josta ne ovat noudettavissa. Varmenteisiin liittyvään tietovarastoon pääsee internetin kautta ja se sijaitsee osoitteessa http://support.partnergate.sonera.com/.*

Tilaaja: *Yhden tai useamman Varmenteen haltijan puolesta toimiva Varmentajan asiakas. Varmenteen haltija voi olla Tilaaja joka toimii omasta puolestaan. [ETSI TS 101 456 v1.2.1]*

Varmenne, Certificate: *Varmenteen haltijan julkinen avain sekä muuta tietoa allekirjoitettuna Varmentajan yksityisellä avaimella siten, että niitä ei voi väärentää. [ISO/IEC 9594-8; ITU-T X.509]*

Varmennepolitiikka, Certificate Policy (CP): *Säännösdokumentti, joka määrittelee varmenteen soveltuvuuden tietylle käyttäjäryhmälle ja / tai tietyntyyppisiin sovelluksiin, joilla on yhteiset tietoturvavaatimukset. [ISO/IEC 9594-8; ITU-T X.509]*

Varmennepolitiikkayksikkö, Policy Authority: *Varmentajan yksikkö, joka määrittelee, hyväksyy ja ylläpitää varmennepolitiikkaa sekä valvoo sovellettuja käytäntöjä.*

Varmennuskäytäntö, Certification Practice Statement (CPS): *Dokumentti käytännöistä, joita Varmentaja noudattaa myöntäessään varmenteita [RFC 2527].*

Varmentaja, Certification Authority (CA): *Osapuoli, johon yksi tai useampi käyttäjä luottaa varmenteiden luomisessa ja myöntämisessä. Varmentaja voi myös mahdollisesti luoda käyttäjien avaimet. [ISO/IEC 9594-8; ITU-T X.509]. Tässä politiikassa Varmentaja on TeliaSonera Finland Oyj.*

Varmenteen hakija: *Henkilö, jolle haetaan varmennetta. Varmenteen myöntämisen jälkeen kutsutaan nimellä Varmenteen haltija.*

TeliaSonera Finland Oyj

Varmenteen haltija: *Varmenteessa mainittua julkista avainta vastaavan yksityisen avaimen (varmenteessa mainittu) haltija. [ETSI TS 101 456 v1.2.1] Varmenteen haltija voi olla myös laite (tietojärjestelmän komponentti tai ohjelmisto joista käytetään jatkossa nimitystä "Laite").*

Varmenteen valmistaja, Certificate Manufacturer (CM): *Osapuoli, joka on vastuussa määritellyin osin Varmentajan allekirjoittamien varmenteiden tai allekirjoituksen luomisvälineen valmistuksesta ja/tai toimituksesta. Sonera PKI:ssa Varmenteen valmistajana on esim. Korttivalmistaja.*

Yksityinen avain: *Varmenteen haltijalle kuuluvan asymmetrisen avainparin se osa, jota vain kyseinen henkilö tai Laite voi käyttää siihen liittyvän aktivointitiedon avulla.*

TeliaSonera Finland Oyj

1 Johdanto

1.1 Yleistä

Varmennuskäytäntö (CPS, Certification Practice Statement) on varmentajan (CA, Certification Authority) kuvaus käytännöistä, joita se noudattaa varmenteita myöntäessään. Tämän varmennuskäytännön tarkoituksena on kuvata menettelytavat, joita Sonera-varmentaja (Sonera Class1 CA, Sonera Class2 CA, Sonera Mobile Class1 CA) käyttää varmenteita myöntäessään ja joita kaikkien varmenteen hakijoiden, tilaajien, haltijoiden ja käyttäjien tulee noudattaa näiden varmenteiden yhteydessä. Tämän varmennuskäytännön rakenne perustuu dokumenttiin RFC 2527 ”Certificate Policy and Certification Practices Framework”.

Varmenteita voidaan käyttää tunnistamiseen sekä kiistämättömyyden, eheyden ja luottamuksellisuuden varmistamiseen.

Varmentaja voi luoda Ali-CA:ita Sonera Class2 CA:n alle huolimatta siitä mitä tässä politiikassa myöhemmin määritellään. Tämän politiikan määräykset ja käytännöt eivät koske Ali-CA varmenteita vaan ainoastaan käyttäjä- ja laitevarmenteita. Ali-CA:n myöntämiä varmenteita koskevat määräykset ja käytännöt määritellään aina Ali-CA:n omassa varmennekäytännössä.

Politiikat, jotka ohjaavat Sonera CA:n (myöhemmin ”Varmentaja”) palveluiden toteuttamista ja ylläpitoa ja määrittelevät säännöt varmenteiden hakemiselle, myöntämiselle ja käytölle, on kuvattu varmennepolitiikoissa: ”TeliaSonera Finland CP-Class1”, ”TeliaSonera Finland CP-Class2” ja ”TeliaSonera Finland Mobiili-CP-1”. Varmentaja myöntää varmenteet kyseisissä varmennepolitiikoissa määriteltyjen turvavaatimusten mukaisesti.

1.2 Dokumentin tunnus

Tämän varmennuskäytännön nimi on “**Sonera CA, Varmennuskäytäntö**” ja sen tunnus on “**TeliaSonera Finland CPS-1 v. 2.2**”. Tätä varmennuskäytäntöä hallinnoi Soneran Varmennepolitiikkayksikkö.

1.3 Osapuolet ja soveltamisala

1.3.1 Varmentaja (CA)

Tämän varmennuskäytännön mukaisesti toimiva Varmentaja on TeliaSonera Finland Oyj. Varmentajan myöntämien varmenteiden Issuer-kentässä on Varmentajan nimenä vaihtoehtoisesti:

Sonera Class1 CA

Sonera Class2 CA

Sonera Mobile Class1 CA

Varmenteiden myöntämisen ja julkaisemisen lisäksi Varmentaja huolehtii myös varmenteiden Sulkupalvelusta ja Sulkulistapalvelusta.

TeliaSonera Finland Oyj

1.3.2 Varmenteen valmistaja

Varmenteen valmistajaksi kutsutaan Varmentajan alihankkijaa, joka on osallisena varmennepalveluiden tuottamisessa jossain muussa kuin Rekisteröijän roolissa. Myös käyttäessään Varmenteen valmistajia alihankkijoinaan Varmentaja on kuitenkin viime kädessä vastuussa varmennepalvelusta kokonaisuutenaan.

1.3.3 Rekisteröijä (RA)

Rekisteröijinä voivat toimia Varmentajan omaan organisaatioon kuuluvat rekisteröintitoimintaan valtuutetut yksiköt, Varmentajan valtuuttamat varmennepalveluiden asiakkaina toimivat asiakasorganisaatiot tai muut Rekisteröijiksi valitut ja valtuutetut organisaatiot, joiden kanssa Varmentaja tekee kirjalliset sopimukset. Näillä sopimuksilla Rekisteröijät velvoitetaan noudattamaan tätä varmennuskäytäntöä omalta osaltaan. Varmentaja kantaa kuitenkin viime kädessä kokonaisvastuun myönnetyistä varmenteista.

Rekisteröintiin liittyvä osuus Varmentajan kokonaisvastuusta voidaan Varmentajan ja Luottavan osapuolen välisellä sopimuksella kuitenkin siirtää Luottavalle osapuolelle silloin, kun tämä toimii myös Rekisteröijänä. Asiakasorganisaatio voi ottaa sopimuksella kantaakseen erikseen määriteltävän osan Varmentajan rekisteröintiin liittyvästä vastuusta silloin, kun Varmenteen hakijat ovat sopimussuhteessa asiakasorganisaatioon ja varmenteiden käyttö liittyy asiakasorganisaation toimintoihin.

1.3.4 Varmenteen haltija

Varmenteen haltija voi olla luonnollinen henkilö, jonka yksinomaiseen käyttöön varmenteen sisältämää julkista avainta vastaava yksityinen avain on tarkoitettu, tai Laite, jolla oleva ohjelmisto pystyy käyttämään Laitteelle tallennettua yksityistä avainta.

1.3.5 Tilaaja

Tilaaja tekee Varmentajan kanssa sopimuksen varmenteen luomisesta ja käyttöönotosta joko itselleen tai edustamalleen luonnolliselle henkilölle tai hallinnassaan olevalle Laitteelle (Varmenteen haltija). Tilaaja vastaa siitä, että Varmenteen haltija noudattaa tässä varmennuskäytännössä määriteltyjä velvoitteita sekä varmennepalvelun ehtoja.

1.3.6 Luottava osapuoli

Luottava osapuoli on asiakasorganisaatio, joka hyödyntää varmenteita yrityksen sisäisen tai ulkoisen toiminnan turvaamisessa. Luottava osapuoli voi olla myös asiakasorganisaation kanssa asioiva yritys, organisaatio tai yksityishenkilö.

1.3.7 Sopimussuhteet

Varmentaja on sopimussuhteessa asiakasorganisaatioon, sekä kaikkiin osapuoliin, jotka suorittavat Varmentajan toimintaan kuuluvia tehtäviä. Sopimuksista tulee käydä selkeästi ilmi osapuolten oikeudet ja velvollisuudet, erityisesti varmennustoiminnan edellyttämät turvavaatimukset.

TeliaSonera Finland Oyj

1.3.8 Soveltamisala

Sonera CA myöntää kolmeen eri luokkaan kuuluvia varmenteita: toimikorttiin tai USB-avaimeen liittyviä tokenvarmenteita, ohjelmistovarmenteita sekä Varmenne-SIM -korttiin liittyviä mobiilivarmenteita. Varmenneluokkaa koskevat käyttötarkoitukset on rajattu tarkemmin kunkin varmenneluokan omassa varmennepolitiikassa.

Varmenteita käytetään mm. seuraavien teknologioiden yhteydessä:

VPN palvelut
SSL
Allekirjoitukset
Tunnistautuminen
Sähköpostisalaus

Tilaajan ja Varmentajan välisessä sopimuksessa saattaa olla avainten käyttötarkoituksiin liittyviä rajoituksia, jotka tulee ottaa huomioon varmenteita käytettäessä.

1.4 Yhteystiedot

Tätä varmennuskäytäntöä hallinnoi Varmentajan Varmennepolitiikkayksikkö.

Varmentajan Varmennepolitiikkayksikkö huolehtii myös siitä että varmennuskäytäntö toteuttaa kaikki varmennepolitiikoissa ”TeliaSonera Finland CP-Class1”, ”TeliaSonera Finland CP-Class2” ja ”TeliaSonera Finland Mobiili-CP-1” määritellyt vaatimukset.

Varmennepolitiikkayksikön yhteystiedot:

TELIASONERA FINLAND OYJ
00051 SONERA
Puhelin: +358 (0) 20401

Yhteyshenkilö varmennuskäytäntöön liittyvissä asioissa:

Sonera CA Tuotepäällikkö
Sähköposti: cainfo@sonera.com
Puhelin: +358 (0) 20401

Asiakaspalvelu: +358 (0) 800 17000 (ma-pe klo 8-21 ja la 9-16.30)
Tekninen asiakaspalvelu (24 h): +358 (0) 800 19101 (ma-pe klo 8-21 ja la 9-16.30)
Sulkupalvelu: +358 (0) 800 156677 (24h)
Internet: http://support.partnergate.sonera.com/

TeliaSonera Finland Oyj

2 Yleiset säännökset

2.1 Velvollisuudet

Osapuolten yleiset velvollisuudet on määritelty varmennepolitiikoissa (kappaleet 2.1.1 – 2.1.4).

Tilaajalle on varmennepolitiikoissa asetettu velvollisuus huolehtia siitä että Varmenteen haltija sitoutuu tälle asetettuihin velvollisuuksiin. Tilaajan tulee ohjeistaa Varmenteen haltijaa seuraavien velovollisuuksien täyttämisessä:

- Varmenteen hakijan tulee rekisteröinnin yhteydessä antaa riittävät ja oikeat tiedot varmenteen hakemista varten.
- Varmenteen haltijan tulee käyttää yksityistä avaintaan vain Tilaajan hyväksymiin tarkoituksiin
- Varmenteen haltijalla on velvollisuus säilyttää yksityinen avaimensa sekä sen aktivointiin tarvittava PIN-koodi sillä tavalla suojattuina etteivät ne katoa, paljastu tai joudu ulkopuolisten käsiin.
- Varmenteen haltijan tulee viipymättä tehdä ilmoitus Tilaajan ohjeistuksen mukaan joko suoraan Varmentajalle tai oman organisaationsa Rekisteröintivastaavalle, jos hän epäilee että hänen yksityinen avaimensa tai PIN-koodinsa saattaa olla jonkun toisen hallussa tai jos hän tietää että varmenteessa olevat tiedot eivät enää päde.
- Jos Varmenteen haltija epäilee tai tietää yksityisen avaimensa tai PIN-koodinsa paljastuneen ulkopuolisille, hänen on lopetettava niiden käyttö välittömästi.

Varmentajan laatima dokumentti ”Soneran varmennepalvelut, Asiakkaan vastuut” sisältää myös Varmenteen haltijoille annettavaa ohjeistusta.

2.2 Vahingonkorvausvastuu

2.2.1 Varmentajan vastuun rajoitukset

Varmentaja ei vastaa oikeustoimista tai muista sitoumuksista, jotka syntyvät varmennetta käytettäessä.

Varmentaja ei vastaa välillisistä vahingoista.

Varmentaja ei vastaa vahingoista, jotka johtuvat ylivoimaisesta esteestä.

Varmentaja ei vastaa mahdollisista sopimuksen tai käyttöehtojen vastaisesta varmenteen käytöstä aiheutuvista vahingoista.

Varmentaja ei vastaa yksityisten avainten tai niiden käyttöön vaadittavien tunnuslukujen paljastumisen seurauksena syntyvistä vahingoista.

Varmentaja ei vastaa yleisten tietoliikenneyhteyksien tai -verkkojen toimimattomuudesta johtuvasta varmennepalveluiden käytön estymisestä.

Mikäli varmennepalveluiden käyttöön tarvittavissa Varmentajan omistamissa välineissä havaitaan virheitä tai puutteellisuuksia, jotka vaikuttavat haitallisesti palveluiden käyttöön, Varmentajalla on oikeus vaihtaa kyseiset välineet.

Varmentaja ei vastaa varmennepalveluiden käyttöön tarvittavien Varmenteen haltijan tai asiakasorganisaation laitteiden tai ohjelmistojen toimivuudesta, turvallisuudesta tai soveltuvuudesta varmennepalveluiden käyttöön.

TeliaSonera Finland Oyj

2.3 Taloudellinen vastuu

Taloudellinen vastuu on kuvattu varmennepolitiikoissa.

2.4 Asiakaspalautteet

Valitusten käsittelyssä noudatetaan Soneran palveluiden yleisiä toimitusehtoja yritysasiakkaille.

2.5 Varmennuskäytännön tulkinta ja täytäntöönpano

2.5.1 Sovellettava laki

Varmennepalveluihin sovelletaan Suomen lakia.

2.5.2 Menettelyt riitatilanteissa

Mikäli asiakasorganisaation ja Varmentajan välillä syntyy varmennepalveluihin liittyviä erimielisyyksiä, ne pyritään ensisijaisesti sopimaan neuvotteluin. Mikäli erimielisyyksistä ei päästä sopimukseen, riita ratkaistaan yksijäsenisessä välimiesmenettelyssä.

2.6 Maksut

Varmennepalveluista peritään asiakasorganisaation ja Varmentajan välisen sopimuksen mukaiset maksut.

Luottavalla osapuolella on kuitenkin pääsy Sulkulistapalveluun veloituksetta.

2.6.1 Maksujen palautukset

Maksujen palautuksissa noudatetaan Soneran palveluiden yleisiä toimitusehtoja yritysasiakkaille. Pääsääntöisesti Varmentaja ei palauta asiakasorganisaation jo maksamia maksuja. Vahingonkorvausvastuisiin liittyvät rajoitukset on mainittu tämän dokumentin kappaleessa 2.2 ”Vahingonkorvausvastuu” varmenteen osalta, ja yleiset rajoitukset on mainittu Soneran palveluiden yleisissä toimitusehdoissa yritysasiakkaille kappaleessa 9.2.

2.7 Tietojen julkaiseminen ja tietovarastot

Julkaistavat tiedot ovat tietovarastossa saatavilla 24 tuntia päivässä, 7 päivänä viikossa, lukuunottamatta tarpeellisia huoltokatkoksia. Varmentaja ei vastaa käyttäjän kokemasta palvelun saatavuudesta, mikäli vika tai katkos ilmenee Varmentajasta riippumattomissa järjestelmissä tai palveluissa.

2.7.1 Varmentajan tiedot ja tietovarastot

Seuraavat varmenteet ovat Luottavien osapuolten saatavilla Varmentajan ylläpitämästä hakemistosta:

- Varmentajan varmenteet,
- voimassa olevat Varmenteen haltijoiden varmenteet, mikäli näin on Tilaajan kanssa sovittu.

TeliaSonera Finland Oyj

Useissa Soneran tietoturvapalveluissa, joissa hyödynnetään varmenteita, palveluntarjoaja huolehtii Luottavan osapuolen puolesta varmenteiden tarkistukset.

Varmentaja julkaisee vamenteiden sulkulistat kappaleen 4.4.5 ”Sulkulistojen julkaisu” mukaisesti LDAP-hakemistossa. Sulkulistojen osoitteet on annettu kappaleessa 4.4.6 ”Sulkulistan tarkistamisvelvollisuus” ja ne löytyvät myös varmenteen CRL Distribution Point -kentästä.

Seuraavat Varmentajan tiedot ja varmennepalvelua koskevat tiedot ovat julkisesti saatavilla internetin kautta osoitteesta http://support.partnergate.sonera.com/:

- voimassa oleva varmennepolitiikka (CP) ja sen edelliset julkaistut versiot
- voimassa oleva varmennuskäytäntö (CPS) ja sen edelliset julkaistut versiot
- dokumentti ”Soneran varmennepalvelut, Asiakkaan vastuut”
- Soneran tietoturvapalveluiden asiakasrekisterin rekisteriseloste
- Varmentajan varmenteet

2.7.2 Tietojen julkaisemisaika

Julkisesti saatavilla olevat tiedot on asetettu saataville pysyvästi. Tietojen päivitys edellä mainitulle Varmentajan www-sivulle suoritetaan välittömästi, kun niihin on tullut muutoksia.

Varmenteet julkaistaan välittömästi niiden myöntämisen jälkeen, mikäli julkaisusta on Tilaajan kanssa sovittu.

Varmenteiden sulkulistat julkaistaan vähintään kerran vuorokaudessa. Sulkulistan voimassaoloaika on 48 tuntia.

2.7.3 Pääsynvalvonta

Varmentajan www-sivut ovat julkisesti saatavilla internetissä. Sulkulista on vapaasti saatavilla Varmentajan LDAP-hakemistosta. Varmenteet, jotka on julkaistu hakemistossa, ovat Luottavien osapuolten saatavilla.

2.8 Toiminnan auditointi

2.8.1 Varmentajan itse suorittamat tarkastukset

Varmentaja valvoo varmennusjärjestelmän lokitietoja seuraamalla sekä satunnaisin tarkastuksin oman toimintansa eri osa-alueiden tietoturvallisuutta. Sisäisessä auditoinnissa voidaan käyttää hyväksi myös Soneran yritysturvallisuusyksikön resursseja. Varmentaja voi myös tarkastaa asiakasorganisaatioissa toimivien Rekisteröijien toimintaa. Mikäli Varmentajan suorittamissa tarkastuksissa ilmenee puutteita, Varmentaja ryhtyy tarvittaviin toimenpiteisiin niiden korjaamiseksi.

Varmentajan alihankkijoilla on käytössä myös omia auditointiohjelmia.

2.8.2 Ulkopuolisen auditoijan suorittama auditointi

Varmentajan toiminta auditoidaan vähintään vuosittain ulkopuolisen auditoijan toimesta. Auditoinnissa selvitetään, toimiiko Varmentaja julkaisemiensa varmennepolitiikan ja varmennuskäytännön mukaisesti ja noudattaako se määrittelemäänsä tietoturvapolitiikkaa. Auditoinnissa käydään läpi kaikki varmennustoiminnan prosessit, Varmentajan käyttämät järjestelmät sekä organisaatio. Auditointi kattaa myös Varmentajan alihankkijoiden kuten Korttivalmistajien ja Rekisteröijien toiminnan lukuun ottamatta

asiakasorganisaatioissa toimivia Rekisteröijiä. Ulkopuolinen auditointi teetetään säännöllisesti sekä aina kun prosesseihin tai järjestelmiin tehdään merkittäviä muutoksia.

Varmentajan alihankkijat käyttävät mm. standardin BS7799 mukaista kolmannen osapuolen suorittamaa auditointia.

2.8.2.1 Auditoija ja vaadittu pätevyys

Varmentajan hyväksymän auditoijan tulee olla riippumaton, tunnettu ja hyvämaineinen alan yritys. Auditoijalta edellytetään riittävää asiantuntemusta ja perehtyneisyyttä PKI-teknologioiden hyödyntämiseen ja varmennustoiminnan auditointiin.

2.8.2.2 Toimenpiteet puutteen havaitsemisen jälkeen

Auditoija toimittaa raportin auditoinnin tuloksista Varmentajalle. Mikäli toiminnassa on havaittu puutteita, Varmentaja ryhtyy toimenpiteisiin niiden korjaamiseksi.

Varmentajan omassa toiminnassa havaittujen puutteiden korjaamiseksi laaditaan suunnitelma, johon sisältyvät korjausaikataulut määräytyvät puutteen vakavuuden ja korjaustoimenpiteen vaatiman ajan perusteella.

Mikäli puutteita on havaittu Varmentajan alihankkijoiden toiminnassa, näistä tiedotetaan asianomaisille ja alihankkijaa edellytetään korjaamaan puutteet kohtuullisen ajan kuluessa.

Mikäli auditoinnista seuraa muutostarpeita varmennepolitiikkaan tai varmennuskäytäntöön, näistä tiedotetaan kyseisen dokumentin kappaleessa 8. kuvattujen menettelyjen mukaisesti.

2.8.2.3 Tuloksista tiedottaminen

Auditoijan antama raportti on tarkoitettu Varmentajan sisäiseen käyttöön. Varmentaja voi tiedottaa alihankkijalle tämän oman toiminnan auditoinnin tuloksista. Raportista voidaan tiedottaa kolmansille osapuolille tai se voidaan julkaista osittain tai kokonaan Varmentajan organisaation johdon päätöksellä.

2.9 Salassapitopolitiikka

2.9.1 Luottamukselliset tiedot

Tilaajia ja Varmenteen haltijoita koskevat tiedot, jotka Varmentaja ja Rekisteröijä saavat rekisteröinnin yhteydessä, ovat luottamuksellista tietoa. Luottamuksellisten tietojen salassapidossa noudatetaan Suomen lakia sekä osapuolten välillä mahdollisesti solmittuja salassapitosopimuksia. Varmentaja luovuttaa varmennustoiminnan yhteydessä kerättyjä ja syntyneitä tietoja Suomen lain sallimissa ja velvoittamissa rajoissa.

2.9.2 Tiedot, joita ei pidetä luottamuksellisina

Varmenteiden sisältämiä tietoja ei pidetä luottamuksellisina tietoina.

Myös sulkulistan sisältämät tiedot ovat julkisia. Sulkulistalla ei julkaista varmenteen haltijan tunnistetietoja, vaan peruutettu varmenne tunnistetaan sen sarjanumeron perusteella.

TeliaSonera Finland Oyj

2.9.3 Tietojen luovutus viranomaisille

Varmentaja luovuttaa varmennustoiminnan yhteydessä kerättyjä ja syntyneitä tietoja viranomaisille ainoastaan Suomen lain sallimissa ja velvoittamissa rajoissa.

2.9.4 Tietojen luovutus Varmenteen haltijalle

Varmenteen haltijalla on oikeus saada häntä koskevia tietoja mm. henkilötietolakiin perustuen.

2.10 Immateriaalioikeudet

Immateriaalioikeudet on kuvattu varmennepolitiikoissa kappaleessa 2.10.

3 Tunnistaminen

3.1 Nimeämiskäytäntö Varmentajan varmenteissa

Tämä varmennuskäytäntö toteuttaa useita eri varmennepolitiikkoja, joista jokaista varten on oma yksikäsitteinen Varmentajan nimi.

Varmentajan varmenteessa Varmentajan yksikäsitteisenä nimenä käytetään sekä ”Issuer”- että ”Subject”–kentässä X.501:n mukaista Distinguished Name (DN) –nimeä joka sisältää seuraavat attribuutit:

- kutsumanimi (commonName, CN),
- organisaatio (organizationName, O)

Attribuuttien tarkka sisältö on kuvattu kussakin varmennepolitiikassa.

3.2 Uuden Varmenteen haltijan rekisteröinti

3.2.1 Varmenteen haltijan nimeäminen

Varmenteessa oleva Varmenteen haltijan nimi voi koostua seuraavista osista:

- kutsumanimi (commonName, CN),
- etunimi (givenName, GN)
- sukunimi (Surname, S)
- sarjanumero (serialNumber, SN),
- organisaatio (organizationName, O),
- organisaatioyksikkö (organizationalUnitName, OU),
- maa (countryName, C),
- paikkakunta (Location),
- valtion nimi (State),

Edellä mainituista osista pakollisia kaikissa varmenteissa ovat CN ja O. Varmentaja vastaa aina o-arvon määrittelystä. Muut varmenteen arvot ovat asiakkaan määriteltävissä.

Varmenteen haltijan nimeen voidaan sisällyttää tarvittaessa myös muita osia.

Kunkin varmennetyypin omassa varmennepolitiikassa on kuvattu tarkemmin nimen osien käyttö.

3.2.2 Nimien merkitykset ja tulkinta

Nimien merkitykset ja tulkinta on kuvattu kunkin varmennetyypin varmennepolitiikassa.

3.2.3 Nimien yksikäsitteisyys

Nimien yksikäsitteisyyteen liittyvät vaatimukset on määritelty varmennepolitiikoissa.

TeliaSonera Finland Oyj

3.2.4 Nimierimielisyyksien ratkaisumenettely

Nimierimielisyyksien ratkaisumenettely on määritelty varmennepolitiikoissa.

3.2.5 Organisaation tunnistaminen

Uusi asiakasorganisaatio tunnistetaan tilauksessa tai sopimuksessa olevien tietojen pohjalta tarkistamalla yrityksen olemassaolo ja Y-tunnus tai vastaava tunniste kolmannen osapuolen ylläpitämästä tietokannasta. Tilauksessa tai sopimuksessa on määriteltynä Tilaajan hallinnollinen yhteyshenkilö, joka määrittelee tarvittavat valtuudet asiakasorganisaatiossa. Yhteyshenkilön aitous varmistetaan soittamalla tälle asiakasorganisaation vaihteen numeron kautta, tai vaihteen puuttuessa johonkin muuhun organisaatiolle kuuluvaan numeroon, joka haetaan kolmannen osapuolen ylläpitämästä luettelosta.

3.2.5.1 Asiakasorganisaatiossa toimivan Rekisteröintivastaavan tunnistaminen

Asiakasorganisaation hallinnollinen yhteyshenkilö voi tilata organisaatiolleen oikeuden myöntää o-arvoltaan organisaatiota kuvaavia ja sovitun mukaisia varmenteita. Tämän jälkeen varmentaja myöntää varmenteita seuraavien ehtojen mukaisesti.

Class 1
Rekisteröintivastaavan tunnistaminen rekisteröintioikeuksia annettaessa suoritetaan asiakasorganisaatiossa. Asiakasorganisaation hallinnollinen yhteyshenkilö voi valtuuttaa rekisteröintivastaavia organisaatioonsa toimittamalla Varmentajalle kirjallisena allekirjoittamansa valtuutuksen Valtuutus sisältää myös Rekisteröintivastaavan allekirjoituksen, mikäli tämä tilaa jatkossa varmenteita käsin allekirjoittamillaan lomakkeilla. Samalla toimitetaan Rekisteröintivastaavan varmennehakemustiedot. Asiakasorganisaation Rekisteröintivastaavalla on oikeus määritellä organisaatioon uusia Rekisteröintivastaavia ja käynnistää näiden varmenteiden haku.

Varmenteen haltijoita rekisteröitäessä Rekisteröintivastaava tunnistetaan joko varmenteiden tilauslomakkeella olevasta allekirjoituksesta tai Sonera Class 1 -varmenteen tai Sonera Mobiilivarmenteen avulla.

Class 2
Rekisteröintivastaavan tunnistaminen rekisteröintioikeuksia annettaessa suoritetaan asiakasorganisaatiossa. Asiakasorganisaation hallinnollinen yhteyshenkilö voi valtuuttaa rekisteröintivastaavia organisaatioonsa toimittamalla Varmentajalle kirjallisena allekirjoittamansa valtuutuksen. Valtuutus sisältää myös rekisteröinti-vastaavan allekirjoituksen, mikäli tämä tilaa jatkossa varmenteita käsin allekirjoittamillaan lomakkeilla. Samalla toimitetaan Rekisteröintivastaavan varmennehakemustiedot (paitsi jos Rekisteröintivastaavan tunnistukseen käytetään pelkkää käyttäjätunnus/salasanayhdistelmää). Asiakasorganisaation Rekisteröintivastaavalla on oikeus määritellä organisaatioon uusia Rekisteröintivastaavia ja käynnistää näiden varmenteiden haku tai hakea näille käyttäjätunnukset ja salasanat.

Varmenteen haltijoita rekisteröitäessä Rekisteröintivastaava tunnistetaan Sonera CA:n myöntämän varmenteen avulla, varmenteiden tilauslomakkeella olevasta allekirjoituksesta tai käyttäjätunnuksen ja salasanan ja mahdollisen kertakäyttösalasanan perusteella. Varmenteen haltijoita rekisteröitäessä voidaan myös käyttää Sonera CA:n tunnistamaa rekisteröintijärjestelmää. Järjestelmän käyttö vaatii rekisteröintivastaavien tunnistamisen.

Mobiilivarmenne
Rekisteröintivastaavan tunnistaminen rekisteröintioikeuksia annettaessa suoritetaan asiakasorganisaatiossa. Organisaation ensimmäiset Rekisteröintivastaavat nimetään ja heidän varmennehakemustietonsa annetaan varmennepalveluiden sopimuksessa. Rekisteröintivastaavalla on oikeus määritellä organisaatioon uusia Rekisteröintivastaavia tai poistaa Rekisteröintivastaavan oikeudet käyttäen Varmentajan toimittamaa työkalua, jolloin hänet tunnistetaan Sonera Mobiilivarmenteen perusteella. Kun Rekisteröintivastaavalle luovutetaan

hänen yksityiset avaimet sisältävä Varmenne-SIM -korttinsa, hänen henkilöllisyytensä tarkistetaan henkilöllisyyden osoittavasta todistuksesta.

Kun valtuutettu Rekisteröintivastaava suorittaa Varmenteen haltijoiden rekisteröintiä, hänet tunnistetaan erikseen jokaisen henkilön rekisteröinnin yhteydessä Sonera Mobiilivarmenteen avulla.

3.2.5.2 Tunnistaminen haettaessa varmennetta Laitteelle

Asiakasorganisaatio voi hakea varmennetta Laitteelle ilman että organisaatiolle on määritelty Rekisteröintivastaavaa. Asiakasorganisaatio ja hallinnollinen yhteyshenkilö tunnistetaan tilauksen tietojen perusteella kuten kappaleen 3.2.5 ”Organisaation tunnistaminen” alussa on kuvattu. Palvelinvarmenteiden osalta tarkistetaan kolmannen osapuolen ylläpitämästä tietokannasta, että tilauksessa mainittu laitteen IP-osoite tai domain-nimi (verkkotunnus) kuuluu tilauksen tehneelle organisaatiolle tai tämän valtuuttamalle palveluntarjoajalle.

Kun Varmentajan omat valtuutetut henkilöt hakevat Soneran tietoturvapalveluiden vaatimia palvelimien käyttämiä laitevarmenteita, tunnistus tapahtuu pääsääntöisesti varmenteen avulla. Vaihtoehtoisesti varmenteen haussa voidaan käyttää Varmentajan sovellusta, jonka käyttöoikeudet on rajattu tietyille henkilöille ja joka edellyttää henkilökohtaisten käyttäjätunnusten ja salasanojen käyttöä.

3.2.6 Varmenteen hakijan henkilöllisyyden ja nimen tarkistaminen

Varmenteen hakijan henkilöllisyyden ja nimen tarkistaminen tapahtuu asiakasorganisaatioissa toimivien Rekisteröintivastaavien toimesta. Rekisteröintivastaavan vastuulla on myös varmistua siitä että Varmenteen hakijalla on asiakasorganisaatiolta saatu oikeus hakea varmennetta. Rekisteröintivastaavilla on velvollisuus noudattaa rekisteröinnissä Varmentajan antamia ohjeita, jotka sisältyvät dokumenttiin ”Soneran varmennepalvelut, Asiakkaan vastuut”.

Class 1 ja Class 2
Henkilöllisyyden ja nimen tarkistamisessa käytetään hyväksi asiakasorganisaation henkilöstöstään tai sopimussuhteessa olevista partnereistaan aiemmin tallentamia tietoja tai Rekisteröintivastaava tarkistaa tiedot Varmenteen hakijan henkilöllisyyden osoittavasta todistuksesta.

Mobiilivarmenne
Rekisteröintivastaava tarkistaa Varmenteen hakijan henkilöllisyyden ja nimen kuvallisesta voimassa olevasta henkilöllisyyden osoittavasta todistuksesta, josta tulee ilmetä sen voimassaolon päättymisajankohta.

3.2.7 Yksityisen avaimen hallussapidon todentaminen

Class 1 ja Class 2
Mikäli Varmentaja ei luo Varmenteen haltijan avainparia vaan se luodaan asiakasorganisaatiossa, Varmentaja voi todentaa yksityisen avaimen hallussapidon tarkistamalla varmennepyynnön mukana tulevan sähköisen allekirjoituksen. Pyyntö hyväksytään vain jos se on allekirjoitettu yksityisellä avaimella, joka vastaa varmennettavaksi pyydettävää julkista avainta.

Mobiilivarmenne
Asiakasorganisaatiossa Rekisteröintivastaava todentaa yksityisen avaimen hallussapidon. Rekisteröinti-vastaava varmistaa Varmenteen hakijan henkilöllisyyden todennettuaan, että tällä on hallussaan yksityisen avaimen sisältävä Varmenne-SIM-kortti, ja käynnistää varmenteen haun kyseistä yksityistä avainta vastaavalle julkiselle avaimelle ja kyseiselle Varmenteen hakijalle.

TeliaSonera Finland Oyj

3.3 Varmenteen uusiminen, uuden avainparin luonti ja tietojen päivitys

Kun varmenne uusitaan, varmennepyynnön/-tilauksen toimittaneen Rekisteröintivastaavan tunnistus tehdään samalla tavalla kuin Varmenteen haltijan ensimmäistä varmennetta haettaessa. Asiakasorganisaatioiden Rekisteröintivastaavilla on myös varmenteita uusittaessa velvollisuus noudattaa rekisteröinnissä dokumenttia ”Soneran varmennepalvelut, Asiakkaan vastuut”.

Class 1
Kun varmenteen voimassaoloaika on päättymässä tai jos varmenteessa olevat tiedot eivät enää päde, varmenne voidaan uusia. Asiakasorganisaation Rekisteröintivastaavan vastuulla on varmistua siitä, että varmenteen uusimiselle ei ole esteitä. Rekisteröintivastaava vastaa myös varmenteeseen tulevien tietojen oikeellisuudesta. Mikäli Varmenteen hakijan tiedot ovat muuttuneet, niiden tarkistus tehdään kuten ensimmäistä varmennetta haettaessa.

Jos on tarpeen luoda uusi avainpari Varmenteen haltijan käyttöön, Varmenteen haltijalle luodaan uusi varmenne. Varmenteen hakijan rekisteröinnissä noudatetaan tällöin samaa prosessia kuin haettaessa ensimmäistä varmennetta.

Class 2
Kun varmenteen voimassaoloaika on päättymässä tai jos varmenteessa olevat tiedot eivät enää päde, varmenne voidaan uusia. Varmenne uusitaan myös silloin, jos on tarpeen luoda Varmenteen haltijalle uusi avainpari.

Mikäli varmenteen uusiminen käynnistetään Asiakasorganisaation Rekisteröintivastaavan toimesta, tämän vastuulla on varmistua siitä, että varmenteen uusimiselle ei ole esteitä. Jos Varmenteen hakijan tiedot ovat muuttuneet, niiden tarkistus tehdään kuten ensimmäistä varmennetta haettaessa.

Kun varmenteen voimassaoloaika on päättymässä, varmenteen uusiminen voidaan käynnistää myös Varmentajan rekisteröintipisteessä. Tällöin rekisteröintipiste tarkistaa, että varmenteen alkuperäinen käyttötarkoitus on vielä olemassa.

Mikäli varmennetta käytetään jonkin Soneran palvelun yhteydessä ja palvelun muutos tai virhe edellyttää uuden varmenteen käyttöönottoa, varmenteen uusiminen voidaan käynnistää myös Varmentajan rekisteröintipisteessä.

Mobiilivarmenne
Kun varmenteen voimassaoloaika on päättymässä, Varmenteen haltijalle voidaan toimittaa uusi Varmenne-SIM -kortti ja avainpari sekä luoda tälle varmenne tai vanhalle avainparille luodaan uusi varmenne. Samoin jos muutoin on tarpeen luoda uusi avainpari Varmenteen haltijan käyttöön tai jos varmenteessa olevat tiedot eivät enää päde, Varmenteen haltijalle luodaan uusi varmenne. Asiakas-organisaation Rekisteröintivastaavan vastuulla on varmistua siitä, että uuden varmenteen luomiselle ei ole esteitä. Rekisteröintivastaava vastaa myös varmenteeseen tulevien tietojen oikeellisuudesta.

3.4 Avainten uusiminen varmenteen peruuttamisen jälkeen

Kun Varmenteen haltijan varmenne on peruutettu ja hän haluaa uuden varmenteen, tämä edellyttää uuden avainparin luomista. Varmenteen hakijan rekisteröinnissä noudatetaan tällöin samaa prosessia kuin haettaessa ensimmäistä varmennetta.

TeliaSonera Finland Oyj

3.5 Peruuttamispyyntö

3.5.1 Varmentajan Sulkupalvelun toteuttama peruuttamispyyntö

Varmenteen haltija tai Tilaaja tai asiakasorganisaatiossa toimiva Rekisteröintivastaava tekee peruuttamispyynnön puhelimitse tai sähköpostilla Sulkupalveluun. Sulkupalvelu tekee takaisinsoiton asiakasorganisaatioon ja kysyy määrätyt tiedot. Näitä tietoja verrataan Varmenteen haltijasta rekisteröinnin yhteydessä tallennettuihin tietoihin ja tarvittaessa Tilaajan tai asiakasorganisaation kanssa tehtyjen sopimusten tietoihin. Mikäli tiedot täsmäävät, varmenne peruutetaan.

Peruuttamispyynnön tekijän tunnistamiseen käytetyt tiedot sekä peruuttamispyynnön vastaanottoaika tallennetaan.

Peruuttamispyyntö voi olla myös jonkin järjestelmän automaattisesti tuottama määrämuotoinen lista Varmenteen haltijoista, joilta poistuu tietyn palvelun käyttöoikeudet, ja palvelun käyttöön liittyvät varmenteet halutaan samalla peruuttaa. Peruuttamispyyntö hyväksytään Sulkupalvelussa, mikäli se täyttää oikeat määrämuotoisuuden vaatimukset ja tulee hyväksytystä osoitteesta. Peruuttamispyyntö tallennetaan.

Joissain tilanteissa, joissa yksityiseen avaimeen kohdistuu tunnistettu väärinkäytön riski tai on ilmeistä, että avainta ei voida oikeutetusti käyttää, voi olla tarpeen peruuttaa varmenne jonkun muun kuin edellä mainittujen pyynnöstä. Tällöin peruuttamispyynnön oikeellisuuden selvittäminen voi vaatia muita tunnistamistapoja. Tapauksissa, joissa luotettavaa tunnistusta ei voida tehdä välittömästi, Varmentaja saattaa kuitenkin asettaa etusijalle varmenteen peruuttamisen riskien vähentämiseksi.

Jos muita tunnistamistapoja käytetään, tunnistamistiedot sekä syy niiden käyttöön tallennetaan.

3.5.2 Asiakasorganisaatiossa toteutettava peruuttamispyyntö

Class 1 ja Class 2
Varmenteen haltija tai Tilaaja pyytää oman organisaationsa Rekisteröintivastaavaa, jolla on myös Sulkupalveluvastaavan oikeudet, peruuttamaan Varmenteen haltijan Varmenteen. Peruuttamis-pyynnön oikeellisuuden varmistaminen on Sulkupalveluvastaavan vastuulla. Asiakasorganisaation Sulkupalveluvastaava tunnistetaan varmenteen perusteella.

Mobiilivarmenne
Mobiilivarmenteen peruuttaminen toteutetaan aina Varmentajan Sulkupalvelun kautta.

3.5.3 Matkapuhelinliittymän sulkupyyntö

Mobiilivarmenne
Varmenteen peruuttamispyynön sijasta asiakas voi pyytää matkapuhelinliittymän sulkua (SAP-tila), jolloin myös varmenteeseen liittyvän yksityisen avaimen käyttö estyy. Matkapuhelinliittymän sulkupyyntö on tunnistettava samoilla menetelmillä kuin varmenteen peruuttamispyyntö.

3.6 Varmenteen käytön tilapäisen eston purkaminen

Jäädytetyn varmenteen palauttamista käyttöön voi pyytää Varmenteen haltija tai asiakasorganisaatiossa toimiva Rekisteröintivastaava. Varmenteen haltijalta tullut pyyntö toteutetaan vasta Rekisteröintivastaavalta saadun vahvistuksen jälkeen. Rekisteröintivastaavalta sähköpostilla tai sähköisellä lomakkeella tullut pyyntö tai vahvistus tunnistetaan sähköisen allekirjoituksen perusteella, tai Rekisteröintivastaavan tunnistaminen

toteutetaan takaisinsoitolla asiakasorganisaatioon ja kysymällä ja tarkistamalla niitä tietoja, joita rekisteröinnin yhteydessä Varmenteen haltijasta tai Rekisteröintivastaavasta on tallennettu tai joita löytyy Tilaajan tai asiakasorganisaation kanssa tehdyistä sopimuksista. Takaisinsoiton yhteydessä pyydetään varmenteen palauttamispyynnöstä kirjallinen vahvistus.

Allekirjoitettu sähköposti, allekirjoitettu sähköinen lomake tai takaisinsoiton yhteydessä Rekisteröintivastaavan tunnistamiseen käytetyt tiedot ja palauttamispyynnön kirjallinen vahvistus tallennetaan.

3.6.1 Matkapuhelinliittymän SAP-tilan purkaminen

Mobiilivarmenne

SAP-tilassa olevan matkapuhelinliittymän palauttamista käyttöön voi pyytää ainoastaan sama henkilö, joka pyysi liittymän sulkua. Pyynnön hyväksynnän perusteena käytetään salasanaa, joka on sovittu asiakkaan kanssa liittymää suljettaessa. Salasana ja henkilön nimi on tallennettu jo sulkua pyydettäessä.

4 Toiminnalliset vaatimukset

4.1 Varmenteen hakeminen

Kun henkilölle tai Laitteelle haetaan varmennetta, sen saanti edellyttää, että tilaava yritys tai organisaatio on Varmentajan asiakasorganisaatio, johon Varmenteen hakija on sopimussuhteessa tai jonka hallinnassa on se Laite, jolle varmennetta haetaan.

Varmennetta haettaessa on annettava kaikki vaadittavat tiedot. Nämä annetaan joko lomakkeella tai käyttäen Varmentajan toimittamia työkaluja.

4.1.1 Varmenteen hakeminen Rekisteröintivastaavalle

Class 1
Asiakasorganisaation ensimmäisen Rekisteröintivastaavan varmenne haetaan toimittamalla Soneralle allekirjoitettu palvelun tilaus sekä tilaukseen sisältyvä tai erillinen allekirjoitettu Rekisteröintivastaavan valtuutus sekä varmennetta varten tarvittavat tiedot. Varmentajan rekisteröintipisteessä tarkistetaan tilauksen ja valtuutusten allekirjoitukset ja että varmennetta varten on annettu riittävät tiedot.

Asiakasorganisaation Rekisteröintivastaavalla on oikeus määritellä organisaatioon uusia Rekisteröinti-vastaavia ja käynnistää näiden varmenteiden haku.

Class 2
Asiakasorganisaation ensimmäisen Rekisteröintivastaavan varmenne haetaan toimittamalla Soneralle allekirjoitettu palvelun tilaus sekä tilaukseen sisältyvä tai erillinen allekirjoitettu Rekisteröintivastaavan valtuutus sekä varmennetta varten tarvittavat tiedot. Varmentajan rekisteröintipisteessä tarkistetaan tilauksen ja valtuutuksen allekirjoitukset ja että varmennetta varten on annettu riittävät tiedot. Rekisteröintipisteessä tehdään asiakasorganisaation Rekisteröintivastaavan esirekisteröinti ja tälle toimitetaan sähköpostitse kertakäyttösalasana ja muut tarvittavat tiedot, joiden avulla hän voi hakea itselleen varmenteen selainohjelmistonsa avulla.

Rekisteröintivastaavalle voidaan esirekisteröinnin yhteydessä myös hakea varmenne valmiiksi Varmentajan rekisteröintipisteessä.

Asiakasorganisaatiossa toimiva Rekisteröintivastaava voi suorittaa organisaation uusien Rekisteröinti-vastaavien esirekisteröinnin, jonka pohjalta Rekisteröintivastaava hakee heille tai he hakevat itse itselleen varmenteet, kuten yllä on kuvattu.

Mobiilivarmenne
Asiakasorganisaation Rekisteröintivastaavalle haetaan varmenne antamalla tarvittavat tiedot allekirjoitetussa varmennepalveluiden sopimuksessa tai toimittamalla tiedot määrämuotoisella allekirjoitetulla lomakkeella Varmentajalle. Varmentaja tarkistaa että kaikki tarvittavat tiedot on annettu.

4.1.2 Varmenteen hakeminen asiakasorganisaation käyttäjälle tai Laitteelle

Varmentaja ei tarkista asiakasorganisaatioiden toimittamien varmennehakemusten tietosisältöä kuin rajoitetusti. Silloin kun varmennehakemus toimitetaan Varmentajan rekisteröintipisteen kautta, rekisteröintipisteessä tarkistetaan, että hakemus sisältää varmenteeseen tulevat tarvittavat tiedot.

TeliaSonera Finland Oyj

Class 1
Varmenne haetaan toimittamalla allekirjoitettu tilaus Soneralle. Tilauksen tulee sisältää varmennetta varten tarvittavat tiedot. Varmentajan rekisteröintipisteessä tarkistetaan allekirjoitus ja että varmennetta varten on annettu riittävät tiedot.

Vaihtoehtoisesti USB-avaimelle tai toimikortille tallennettavaa varmennetta voidaan hakea suoraan asiakasorganisaation Rekisteröintivastaavan toimesta ilman Varmentajan rekisteröintipisteen toimenpiteitä. Varmenne haetaan käyttämällä hyväksi Varmentajan toimittamaa työkalua, joka edellyttää Rekisteröintivastaavan tunnistusta varmenteen avulla.

Class 2 henkilövarmenteet
Asiakasorganisaation Rekisteröintivastaava voi hakea henkilön käyttöön tulevaa varmennetta joko Varmentajan rekisteröintipisteen kautta tai suoraan varmennusjärjestelmästä Varmentajan toimittamien työkalujen avulla.

Kun varmenne haetaan Varmentajan rekisteröintipisteen kautta, sinne toimitetaan varmennetta varten tarvittavat tiedot sisältävä allekirjoitettu tilaus. Varmentajan rekisteröintipisteessä tarkistetaan allekirjoitus ja että varmennetta varten on annettu riittävät tiedot sekä suoritetaan Varmenteen hakijan esirekisteröinti. Varsinaisen varmenteen haku voidaan suorittaa Varmentajan rekisteröintipisteessä, tai vaihtoehtoisesti hakua varten tarvittavat ohjeet sekä kertakäyttösalasana toimitetaan tilauksen mukaisesti joko Varmenteen hakijalle suoraan tai asiakasorganisaation Rekisteröintivastaavalle.

Poikkeuksen edelliseen muodostavat vakioerissä toimitettavat varmenteet, joissa Varmenteen haltijan nimessä on kutsumanimenä pseudonyymi (ns. pakettitoimitukset). Asiakasorganisaation yhdyshenkilö toimittaa varmenteista kirjallisen tilauksen, joka on yhdyshenkilön allekirjoittama. Tilauksen sisältämät tarpeelliset tiedot siirretään Varmentajan rekisteröintipisteeseen, jossa Rekisteröintivastaava hakee varmenteet.

Kun varmenne haetaan suoraan varmennusjärjestelmästä, asiakasorganisaation Rekisteröintivastaava suorittaa henkilön esirekisteröinnin ja hakee hänelle varmenteen samalla tavoin kuin organisaationsa uudelle Rekisteröintivastaavalle (ks. kappale 4.1.1 ”Varmenteen hakeminen Rekisteröintivastaavalle”), tai henkilö voi esirekisteröinnin jälkeen itse hakea itselleen varmenteen saamansa kertakäyttösalasanan avulla.

Class 2 laitevarmenteet
Laitevarmennetta (SSL-palvelinvarmenne) haetaan täyttämällä asiakasorganisaatiossa lomake, joka on julkisesti saatavilla osoitteen https://partnergate.sonera.com/ kautta. Lomakkeeseen tulee liittää CSR-pyyntö, joka on Laitteen muodostama määrämuotoinen varmennepyyntö. Täytetyt hakulomakkeet ohjautuvat Varmentajan rekisteröintipisteeseen, jossa niiden sisältämien tietojen riittävyys tarkistetaan.

Asiakasorganisaation Rekisteröintivastaavalle voidaan myös antaa oikeus hakea Laitevarmenteita (SSL-palvelinvarmenne) suoraan varmennusjärjestelmästä Varmentajan toimittaman työkalun avulla. Tilaaja määrittelee IP-osoiteavaruuden tai domainit (verkkotunnukset), joihin oikeus kohdistuu, ja Varmentaja tarkistaa, että ne on rekisteröity kyseiselle Tilaajalle.

Soneran tietoturvapalveluiden vaatimat palvelimien käyttämät laitevarmenteet voidaan hakea Varmentajan rekisteröintipisteen kautta, tai ne haetaan Varmentajan omien valtuutettujen henkilöiden toimesta. Rekisteröintipisteen kautta haettaessa sinne toimitetaan tilaus, joka käsitellään kuten SSL-palvelinvarmennetilaus. Varmentajan omat henkilöt voivat hakea varmenteen silloin, kun se kuuluu tietoturvapalvelun toimitukseen eikä siitä tule erillistä tilausta asiakasorganisaatiolta. Varmentajan oma henkilöstö hakee laitevarmenteita vain Soneran hallinnoimille laitteille. Varmenne haetaan Varmentajan omia työkaluja käyttäen.

Muut laitevarmenteet (esim. työasemavarmenne) käsitellään kuten henkilövarmenteet.

Mobiilivarmenne
Rekisteröintivastaava tarkistaa Varmenteen hakijan henkilöllisyyden ja nimen virallisesta kuvallisesta henkilötodistuksesta Varmenteen hakijan ollessa henkilökohtaisesti paikalla. Rekisteröintivastaava luovuttaa

Varmenteen hakijalle uuden Varmenne-SIM -kortin ja sillä olevien yksityisten avainten käyttöön tarvittavat tunnusluvut, mikäli näitä ei ole luovutettu jo aikaisemmin. Tämän jälkeen Rekisteröintivastaava käynnistää varmenteen haun varmennusjärjestelmästä Varmentajan toimittaman työkalun avulla.

4.1.3 Testi- tai pilot-varmenteen hakeminen

Class 1 ja Class 2
Varmentaja on antanut muutamalle palveluksessaan olevalle henkilölle erikoisvaltuudet hakea testivarmenteita sellaisia testejä varten, jotka on välttämätöntä toteuttaa tuotantojärjestelmässä. Testivarmenteen hakija tunnistetaan varmenteen perusteella. Testivarmenteen Subject-kentän sisällöstä ilmenee jollain seuraavista tavoista, että kyseessä on testivarmenne:

- organisaatio-kentän sisältönä on sana ”Testi” (ensisijainen tapa),
- kutsumanimi-kenttä sisältää sanan ”testi”,
- jokin muu kenttä sisältää sanan ”testi”.

Testivarmenne on voimassa enintään 7 vuorokautta tai se peruutetaan aina viimeistään 7 vuorokauden kuluttua sen voimaantulosta. Mikäli ilmenee testitilanne, jossa varmenteen sisällössä ei voida ilmaista, että kyseessä on testivarmenne, se on peruutettava välittömästi testin jälkeen.

Varmentaja on antanut muutamalle palveluksessaan olevalle henkilölle erikoisvaltuudet hakea varmenteita Soneran tietoturvapalveluiden pilotointivaiheessa, ennen kuin rekisteröintitoiminta on siirretty Varmentajan rekisteröintipisteen vastuulle. Pilot-varmenteen hakija tunnistetaan varmenteen perusteella. Pilot-varmenteiden hakemisessa noudatetaan samoja vaatimuksia kuin tuotantovaiheen varmenteiden hakemisessa.

Mobiilivarmenne
Testejä varten tarvittavat Mobiilivarmenteet haetaan samojen Rekisteröintivastaavien toimesta ja samoin menettelyin kuin tuotantovarmenteet. Testivarmenteen kentistä tulee löytyä sana ”test”. Testivarmenne peruutetaan välittömästi, kun sitä ei enää tarvita testausta varten.

4.2 Varmenteen myöntäminen

Varmennusjärjestelmä hyväksyy vain sellaiset varmennepyynnöt, joiden alkuperä voidaan tunnistaa sähköisestä allekirjoituksesta.

Varmenteen haltijoiden nimien yksikäsitteisyys varmistetaan kaksivaiheisesti. Nimi sisältää sekä organisaation nimen että Varmenteen haltijan nimen. Varmentajan järjestelmä sallii ainoastaan yksikäsitteiset organisaationimet. Asiakasorganisaatio ei pysty itse muuttamaan organisaationimeään, jonka Varmentaja on järjestelmäänsä tallentanut. Asiakasorganisaatiot vastaavat omien käyttäjiensä nimien yksikäsitteisyydestä.

Kun asiakasorganisaation Rekisteröintivastaava luovuttaa haetun varmenteen, yksityisen allekirjoitusavaimen ja siihen liittyvän PIN-koodin Varmenteen haltijalle, hän on velvollinen noudattamaan dokumentissa ”Soneran varmennepalvelut, Asiakkaan vastuut” annettuja ohjeita.

Class 1
Toimikortille tallennettavan varmenteen tapauksessa Varmentajan rekisteröintipiste toimittaa rekisteröintitiedot sisältävän tilauksen salattuna ja allekirjoitettuna Korttivalmistajalle, joka valmistaa kortin ja luo avainparin. Korttivalmistaja toimittaa varmennepyynnön varmennusjärjestelmään salattuna ja allekirjoitettuna. Varmentaja luo varmenteen, jonka korttitehdas tallentaa kortille. Korttivalmistaja toimittaa kortit postitse tilauksessa annettuun osoitteeseen, joka voi olla Varmenteen haltijan tai Rekisteröintivastaavan osoite.

Kortilla oleviin yksityisiin avaimiin liittyvät PIN- ja PUK-koodit toimitetaan erillisinä lähetyksinä postitse tilauksen mukaisesti.

Vaihtoehtoisesti asiakasorganisaation Rekisteröintivastaava luo toimikortille tallennettuja avainpareja hyväksi käyttäen varmennepyynnöt ja toimittaa ne varmennusjärjestelmään allekirjoitettuina ja salattuina Varmentajan toimittaman työkalun avulla. Avainparit voivat olla toimikortille valmiiksi tallennettuina tai ne luodaan varmenteiden hakemisen yhteydessä. Varmentaja luo varmenteet, jotka asiakasorganisaation Rekisteröintivastaava tallentaa toimikortille.

USB-avaimelle tallennettavan varmenteen tapauksessa Varmentajan rekisteröintipiste luo avainparin ja toimittaa varmennepyynnön varmennusjärjestelmään allekirjoitettuna ja salattuna. Varmentaja luo varmenteen, joka Varmentajan rekisteröintipisteessä tallennetaan USB-avaimelle. USB-avain toimitetaan asiakasorganisaation Rekisteröintivastaavalle kirjattuna kirjeenä, ja PIN-koodi suojausohjeineen sähköpostitse.

Vaihtoehtoisesti asiakasorganisaation Rekisteröintivastaava luo USB-avaimelle avainparin ja toimittaa varmennepyynnön varmennusjärjestelmään allekirjoitettuna ja salattuna Varmentajan toimittaman työkalun avulla. Varmentaja luo varmenteen, jonka asiakasorganisaation Rekisteröintivastaava tallentaa USB-avaimelle.

Class 2
Henkilön käyttöön tuleva avainpari voidaan luoda varmennusjärjestelmässä, Varmentajan rekisteröintipisteessä tai sen luo asiakasorganisaation Rekisteröintivastaava tai Varmenteen hakija itse. Avainparin luonnin yhteydessä toimitetaan varmennepyyntö varmennusjärjestelmään salattuna ja allekirjoitettuna. Varmentaja luo varmenteen ja palauttaa sen varmennepyynnön toimittajalle. Mikäli varmennepyyntö toimitettiin Varmentajan rekisteröintipisteestä, varmenne ja siihen liittyvä yksityinen avain toimitetaan sähköpostitse asiakasorganisaation Rekisteröintivastaavalle tai pakettitoimitusten tapauksessa (vakioerissä toimitettavat varmenteet, joissa Varmenteen haltijan nimessä on kutsumanimenä pseudonyymi) tilauksessa ilmoitettuun sähköpostiosoitteeseen. PIN-koodit toimitetaan erikseen toista kanavaa pitkin. Mikäli avainpari on luotu varmennusjärjestelmässä se toimitetaan asiakkaalle suojattuna PKCS12 muodossa.

Varmentaja luo laitevarmenteen varmennepyynnön sisältämien tietojen mukaisesti. Mikäli varmennepyyntö varmennusjärjestelmään toimitettiin Varmentajan rekisteröintipisteen kautta, rekisteröintipiste toimittaa varmenteen sähköpostitse asiakasorganisaation yhteyshenkilölle asennettavaksi laitteeseen tai rekisteröintipiste toimittaa yhteyshenkilölle web-linkin varmenteen noutamiseksi. Kun on kyseessä Soneran tietoturvapalvelun vaatima palvelimen käyttämä laitevarmenne, jonka hakee Varmentajan henkilöstö, se myös asennetaan laitteelle Varmentajan oman henkilöstön toimesta.

Mobiilivarmenne
Varmentaja luo varmenteen varmennepyynnön sisältämien tietojen mukaisesti.

Varmenteen hakija saa matkapuhelimeensa tiedon myönnetystä varmenteesta.

4.3 Varmenteen hyväksyminen

Varmenteen haltijan, tai Laitteille haettavien varmenteiden tapauksessa Tilaajan, katsotaan hyväksyneen varmenteen, kun siihen liittyvää yksityistä avainta on käytetty tai kun varmenne on asennettu työasemaan tai palvelimelle.

TeliaSonera Finland Oyj

4.4 Varmenteen peruuttaminen ja jäädyttäminen

4.4.1 Peruuttamisolosuhteet

Varmenne tulee peruuttaa tai jäädyttää (eli peruuttaa toistaiseksi) seuraavissa olosuhteissa:

- Varmenteen haltija tai Tilaaja pyytää varmenteen peruuttamista (mistä tahansa syystä)
- Varmenteen haltijan yksityinen avain on kadonnut, anastettu tai paljastunut
- Varmenteen haltija käyttää yksityistä avaintaan vastoin sen käyttötarkoitusta
- varmennetta ei ole myönnetty asianomaisen varmennepolitiikan tai tämän varmennuskäytännön mukaisesti
- Varmenteen haltija tai Tilaaja rikkoo oleellisesti Varmentajan kanssa tehtyä sopimusta
- Varmenteen haltija kuolee

Varmenne voidaan peruuttaa tai jäädyttää myös seuraavissa olosuhteissa

- Epäillään että Varmenteen haltijan yksityinen avain on kadonnut, anastettu tai paljastunut
- Varmenteen haltija tai Tilaaja rikkoo Varmentajan kanssa tehtyä sopimusta
- Varmenteen peruuttamiseen on joku muu erityinen syy

Sonera Mobiilivarmenteen peruuttamisen sijasta matkapuhelinliittymä voidaan pyynnöstä sulkea toistaiseksi (SAP-tila) varmennepolitiikassa ”TeliaSonera Finland Mobiili-CP-1” kuvatuissa olosuhteissa. Matkapuhelinliittymän ollessa SAP-tilassa Varmenne-SIM -kortille tallennettujen yksityisten avainten käyttö estyy.

4.4.2 Kuka voi pyytää peruuttamista

Varmenteen peruuttamista voi pyytää pääsääntöisesti ainoastaan Varmenteen haltija, asiakasorganisaation Rekisteröintivastaava tai Tilaajan muu yhteyshenkilö. Peruuttamisen voi panna alulle kuitenkin myös Varmentaja perustuen minkä tahansa osapuolen esille tuomaan luotettavaan ja pätevään tietoon, joka viittaa kappaleen 4.4.1. ” Peruuttamisolosuhteet” mukaisiin peruuttamisolosuhteisiin.

Matkapuhelinliittymän tilapäistä sulkemista (SAP-tila) voivat pyytää vain Tilaaja, asiakas-organisaation Rekisteröintivastaava tai Varmenteen haltija.

4.4.3 Peruuttamispyyntöjen käsittely

4.4.3.1 Peruuttamispyynnön ajanhetken vaikutus

Varmentaja ottaa peruuttamispyyntöjä vastaan 24 tuntia vuorokaudessa 7 päivänä viikossa.

Varmenteen haltijan tai Tilaajan tulee välittömästi ilmoittaa Sulkupalveluun suoraan tai asiakasorganisaation Rekisteröintivastaavan kautta, kun ilmenee peruste varmenteen peruuttamiselle. Myös Rekisteröintivastaavan on ilmoitettava Sulkupalveluun välittömästi, kun hänen tietoonsa tulee peruste varmenteen peruuttamiselle.

Varmentaja ei vastaa Varmenteen haltijan yksityisen avaimen oikeudettomasta käytöstä aiheutuneesta vahingosta. Varmentaja vastaa peruuttamistiedon julkaisemisesta sulkulistalla tässä varmennuskäytännössä ilmoitettujen periaatteiden mukaisesti.

4.4.3.2 Peruuttamispyynnön toteuttaminen

Sulkupalvelussa vastaanotettavien varmenteiden peruuttamispyyntöjen tekijät tunnistetaan kappaleen 3.5 ”Peruuttamispyyntö” mukaisesti.

Varmenteet peruutetaan pysyvästi tai jäädytetään eli peruutetaan toistaiseksi asianmukaisen sulkupyynnön vastaanoton jälkeen. Jäädytetyt varmenteet peruutetaan lopullisesti viimeistään 6 kuukauden kuluttua jäädyttämisestä, ellei niitä ole palautettu käyttöön.

Pyynnöt koskien matkapuhelinliittymien sulkemista toistaiseksi vastaanotetaan Soneran matkapuhelinasiakkaiden asiakaspalvelussa. Matkapuhelin asetetaan SAP-tilaan viipymättä, kun pyyntö on vastaanotettu, pyytäjä tunnistettu ja pyyntö todettu luvalliseksi. Varmentaja voi lisäksi peruuttaa tai jäädyttää varmenteen, mikäli katsoo olosuhteiden tätä vaativan.

4.4.4 Varmenteen jäädyttäminen

Ks kappale 4.4.3.2 ”Peruuttamispyynnön toteuttaminen”.

4.4.5 Sulkulistojen julkaisu

Sulkulistapalvelu toteutetaan julkaisemalla Varmentajan sähköisesti allekirjoittamat sulkulistat julkisessa hakemistossa. Seuraavia sääntöjä noudatetaan:

- Uusi sulkulista julkaistaan hakemistossa **vähintään 24 tunnin** välein.
- Jokainen sulkulista on voimassa **neljäkymmentäkahdeksan (48) tuntia**.

Sulkulista on saatavilla hakemistosta 24 tuntia päivässä, 7 päivää viikossa, lukuun ottamatta tarpeellisia huoltokatkoksia. Varmentaja ei vastaa käyttäjän kokemasta palvelun saatavuudesta, mikäli vika tai katkos ilmenee Varmentajasta riippumattomissa järjestelmissä tai palveluissa.

Hakemistossa saattaa olla yhtä aikaa saatavana useita voimassa olevia sulkulistoja. Näistä viimeisimmäksi julkaistu sisältää ajantasaisimmat tiedot.

4.4.6 Sulkulistan tarkistamisvelvollisuus

Ennen varmenteeseen luottamista Luottavan osapuolen on varmistettava, että varmennetta ei ole asetettu sulkulistalle. Varmenteeseen ei voida riittävin perustein luottaa, jos Luottava osapuoli ei noudata huolellisesti seuraavia sulkulistatiedon tarkistusmenettelyjä:

- Luottavan osapuolen, joka hakee sulkulistan hakemistosta, tulee varmistaa sulkulistan aitous tarkistamalla sen digitaalinen allekirjoitus ja siihen liittyvä varmennuspolku.
- Luottavan osapuolen tulee myös tarkistaa sulkulistan voimassaoloaika varmistuakseen siitä että sulkulistan tieto on ajanmukaista.
- Varmenteita voidaan tallentaa paikallisesti Luottavan osapuolen järjestelmään, mutta ennen käyttöä jokaisen tällaisen varmenteen senhetkinen tila tulee tarkistaa mahdollisen peruuttamisen osalta.
- Jos voimassa olevaa sulkulistatietoa ei ole saatavissa järjestelmä- tai palveluhäiriön takia, yhteenkään varmenteeseen ei pidä luottaa. Varmenteen hyväksyminen vastoin tätä ehtoa tapahtuu Luottavan osapuolen omalla riskillä.

Sulkulistat löytyvät alla olevista osoitteista

Class 1
ldap://194.252.124.241:389/cn=Sonera%20Class1%20CA,o=Sonera,c=FI?certificaterevocationlist;binary

TeliaSonera Finland Oyj

Class 2
ldap://194.252.124.241:389/cn=Sonera%20Class2%20CA,o=Sonera,c=FI?certificaterevocationlist;binary

Mobiilivarmenne:
ldap://194.252.124.241:389/cn=Sonera%20Mobile%20Class1%20CA,o=Sonera,c=FI?certificaterevocationlist;binary

Luottava osapuoli voi hankkia sulkulistojen tarkistuksen palveluna, joka noudattaa yllä olevia sulkulistatiedon tarkistusmenettelyjä.

4.5 Varmenteen käytön tilapäisen eston purkaminen

Varmenteen haltija tai asiakasorganisaatiossa toimiva Rekisteröintivastaava voivat pyytää jäädytetyn varmenteen käyttöön palauttamista. Jos palauttamista pyytää Varmenteen haltija, palauttamiseen vaaditaan vahvistus Rekisteröintivastaavalta. Rekisteröintivastaavan tunnistus tehdään kappaleen 3.6 ”Varmenteen käytön tilapäisen eston purkaminen” mukaisesti.

Varmenteen palauttamispyynnön käsittelee ja hyväksyy Varmentajan henkilö, joka on erikseen valtuutettu tähän tehtävään. Sulkupalvelun on varmistettava ennen palautuspyynnön toteuttamista, että pyyntö tulee Varmentajan valtuuttamalta henkilöltä.

Asiakasorganisaation tulee toimittaa Varmentajalle kirjallisena (sähköpostina, sähköisellä lomakkeella tai faxina) varmenteen palauttamispyyntö tai sen vahvistus, joka tallennetaan vastaanottoaikoineen sekä Rekisteröintivastaavan tunnistukseen käytettyine tietoineen. Samoin tallennetaan Sulkupalveluun toteutusta varten toimitettu pyyntö seuraavine tietoineen: pyynnön sisältö, pyynnön vastaanottoaika, pyynnön lähettäneen Varmentajan valtuutetun henkilön nimi sekä palautuksen toteutusaika.

4.5.1 Matkapuhelinliittymän SAP-tilan purkaminen

Mobiilivarmenne
Pyyntö SAP-tilassa olevan matkapuhelinliittymän käyttöön palauttamisesta vastaanotetaan puhelimitse Soneran matkapuhelinasiakkaiden asiakaspalvelussa. Pyyntö voidaan hyväksyä vain siltä henkilöltä, jolta otettiin vastaan liittymää koskeva tilapäinen sulkupyyntö. Hyväksyntä suoritetaan niiden tietojen perusteella, joita tallennettiin vastaanotettaessa sulkupyyntö, ks. kappale 3.5.1 ”Matkapuhelinliittymän sulkupyyntö”.

Matkapuhelinliittymän käyttöön palauttamista pyytäneen henkilön nimi, käytetty salasana sekä SAP-tilan purkuaika tallennetaan.

4.6 Tietoturvallisuuden valvonta

4.6.1 Tallennettavat tiedot

Varmentaja tallentaa automaattisesti tai manuaalisesti seuraavat oleelliset varmennustoimintaan liittyvät tiedot:

CA-avaimen elinkaareen liittyvät tiedot

- avaimen luonti, varmuuskopiointi, palautus ja tuhoaminen
- salausteknisen laitteen elinkaareen liittyvät ylläpitotapahtumat

Varmentajan ja Varmenteen haltijoiden varmenteiden elinkaareen liittyvät ylläpitotapahtumat

- varmennehakemukset ja -pyynnöt, varmenteiden uusimispyynnöt jo käytössä olleille tai uusille avaimille
- varmenteiden peruuttamiset ja jäädyttämiset
- jäädytettyjen varmenteiden käyttöön palauttamiset
- varmenteiden luomiset
- sulkulistojen luomiset

Tietoturvallisuuden ylläpitoon liittyvät tapahtumat

- Varmentajan varmenteiden hakua varten toimittamilla työkaluilla suoritetut tapahtumat
- Varmentajan henkilöstön suorittamat varmennusjärjestelmään tai turvajärjestelmiin kohdistuvat toimenpiteet, mm. ohjelmistojen, laitteiden ja päivitysten asennukset, palautukset, järjestelmien alasajot ja uudelleenkäynnistykset sekä järjestelmän asetusten muutokset
- järjestelmien kaatumiset, laitteistoviat ja muut poikkeamat järjestelmissä
- reitittimien ja palomuurien ja hyökkäyksenhavaitsemisjärjestelmien tapahtumat
- kulunvalvontatapahtumat varmennusjärjestelmän tiloihin.

Tallennettaviin tietoihin sisältyy tietojen tyyppi, päivämäärä ja kellonaika sekä automaattisesti tallentuviin lokeihin juokseva numero ja lokia tuottavan järjestelmän tunniste.

Varmentajan rekisteröintipisteessä tallennetaan:

- asiakasorganisaatioiden Rekisteröintivastaavien valtuutuslomakkeet
- asiakasorganisaatioista tulleet varmennetilaukset, joissa on tilaavan Rekisteröintivastaavan nimi
- tarkistukset, jotka tehdään kolmansien osapuolten ylläpitämistä tietokannoista.

Sulkupalvelussa tallennetaan peruuttamispyyntöihin liittyen:

- peruuttamista pyytävän henkilön tiedot
- peruuttamista pyytävän henkilön tunnistamistapa
- pyynnön vastaanottoaika
- tiedot varmenteesta, joka halutaan peruuttaa.

4.6.2 Lokitietojen seuranta

Merkittäviä turvallisuuteen ja toimintaan liittyviä lokeja seurataan säännöllisesti Varmentajan henkilöstön toimesta.

Järjestelmien tuottamien hälytysten perusteella suoritetaan lokien läpikäyntiä epäilyttävien tai poikkeavien tapahtumien selvittämiseksi.

4.6.3 Lokitietojen säilytysaika

Varmennusjärjestelmän lokitietoja säilytetään vähintään vuoden ajan niiden syntymisestä, ja tiedot arkistoidaan kappaleessa 4.7.2 ”Arkiston säilytysaika” mainituksi ajaksi.

Varmentajan muiden järjestelmien tuottamia lokitietoja säilytetään järjestelmissä itsessään vähintään 10 päivän ajan niiden syntymisestä. Lisäksi lokitietoja voidaan siirtää myös erilliselle lokipalvelimelle säilytettäväksi. Järjestelmästä riippuen lokitieto viedään sellaisenaan tai prosessoituna toiselle tallennusmedialle arkistointia varten.

4.6.4 Lokitietojen suojaus

Manuaalisesti tallennettavat lokit sekä Varmentajan järjestelmien automaattisesti tuottamat lokit on suojattu muuttamiselta, tuhoamiselta ja oikeudettomalta lukemiselta järjestelmien käyttövaltuushallinnalla ja kulunvalvonnalla.

Varmennusjärjestelmän lokitiedot on suojattu digitaalisella allekirjoituksella.

4.6.5 Lokitietojen varmistus

Varmennusjärjestelmän lokitiedoista otetaan säännöllisesti erikseen määriteltyjen aikataulujen mukaisesti varmuuskopiot.

Muiden varmentajan järjestelmien tuottamien lokitietojen varmistuskäytäntö riippuu järjestelmästä ja lokitietojen kriittisyydestä. Oleellisimmista lokitiedoista otetaan säännöllisesti varmuuskopiot.

4.6.6 Lokitietojen keruujärjestelmä

Varmentajan järjestelmät tukevat lokitietojen keräystä. Tietyt tuotantojärjestelmälle tehtävät hallintatapahtumat, esim. järjestelmän muutokset ja päivitykset sekä CA-avaimiin liittyvät hallintatapahtumat kirjataan käsin erilliseen lokiin.

Varmentajan järjestelmissä automaattisesti syntyvät lokitiedot tallennetaan sovellus-, verkkolaite- ja käyttöjärjestelmätasolla. Manuaaliset lokit tuotetaan pöytäkirjoina fyysisessä tai sähköisessä muodossa Varmentajan henkilöstön toimesta.

4.6.7 Järjestelmien haavoittuvuuden testaus

Varmentaja testaa säännöllisesti kriittisten järjestelmiensä haavoittuvuutta ulkopuolisten suorittamien tunkeutumisyritysten varalta. Testaustulosten perusteella päivitetään tarvittaessa palomuurien ja muiden järjestelmien konfiguraatioita sekä toimintapolitiikkoja ja käytäntöjä.

4.7 Tietojen arkistointi

4.7.1 Arkistoitavat tiedot

Varmentaja arkistoi kappaleessa 4.6.1 ”Tallennettavat tiedot” kuvatuista lokitiedoista kriittisimmät, mm. kaikki varmennusjärjestelmän tuottamat lokit sekä manuaalisesti syntyvät varmennus-järjestelmään kohdistuvista toimenpiteistä tehdyt lokit.

Edellä mainittujen lokitietojen lisäksi vähintään alla olevat tiedot arkistoidaan:

- asiakasorganisaatioiden kanssa tehdyt sopimukset,
- asiakasorganisaatioista vastaanotetut varmennehakemukset ja –tilaukset,
- luodut varmenteet,
- Sulkupalvelun vastaanottamat varmenteiden peruuttamispyynnöt,
- Varmentajan vastaanottamat pyynnöt jäädytettyjen (toistaiseksi peruutettujen) varmenteiden palauttamisesta käyttöön,
- varmenteiden peruuttamiset,

- kaikki Varmentajan julkaisemat varmennepolitiikkaversiot,
- kaikki Varmentajan julkaisemat varmennuskäytäntöversiot,
- raportit ulkopuolisten auditoijien suorittamista auditoinneista.

Tietoja voidaan arkistoida sekä sähköisessä muodossa että fyysisinä dokumentteina.

4.7.2 Arkiston säilytysaika

Kaikki kappaleessa 4.7.1 ”Arkistoitavat tiedot” mainitut tiedot arkistoidaan vähintään kolmen (3) vuoden ajaksi niiden syntymishetkestä laskettuna.

Julkaistut varmenteet ja niihin liittyvät rekisteröintitiedot sekä mahdolliset peruuttamistiedotarkistoidaan vähintään kolmen (3) vuoden ajaksi varmenteen voimassaoloajan päättymisestä laskettuna.

Varmentaja ei kuitenkaan takaa arkistojen säilytystä sen jälkeen kun Varmentajan toiminta on päättynyt.

4.7.3 Arkiston suojaus

Arkistot, jotka sisältävät varmennusjärjestelmän tuottamat varmenteiden luomiseen ja peruuttamiseen liittyvät tiedot sekä itse varmenteet, sijaitsevat kulunvalvonnalla suojatuissa paloturvallisissa tiloissa ja ne on suojattu sähköisellä allekirjoituksella. Samoissa tiloissa arkistoidaan myös järjestelmän muutostiedot ja palvelutapahtumat sisältävät arkistot.

Muiden varmentajan järjestelmien tuottamat arkistoitavat tiedot arkistoidaan kulunvalvonnalla suojatuissa tiloissa joko lukollisessa kaapissa tai kassakaapissa riippuen tiedon kriittisyydestä.

4.7.3.1 Arkistoitujen tietojen aikaleimauksen vaatimukset

Arkistoidut tiedot eivät sisällä varsinaista aikaleimaa. Kaikki varmennusjärjestelmän tuottamat lokit sisältävät päivämäärä- ja kelloaikatiedon. Aika synkronoidaan ulkopuolisen UTC-aikalähteen kanssa.

Myös muiden Varmentajan järjestelmien tuottamat lokit sisältävät päivämäärä- ja kellonaikatiedon. Osassa näitä järjestelmiä aika synkronoidaan ulkopuolisen UTC-aikalähteen kanssa.

4.7.4 Arkiston varmistus

Varmennusjärjestelmän tuottamista arkistotiedoista otetaan varmuuskopiot tiedon häviämisen tai tuhoutumisen varalta, jotta varsinaisen arkiston tuhoutuessa tiedot voidaan palauttaa varmuuskopioista.

4.7.5 Arkistotiedon saanti- ja tarkistamismenettelyt

Arkistotietoja säilytetään siten, että vain valtuutetut Varmentajan henkilöt voivat päästä niihin käsiksi. Arkistotietojen katseluun oikeutettuja ovat ne henkilöt, jotka suorittavat kappaleen 2.8 ”Toiminnan auditointi” mukaista auditointia. Muutoin tietoja toimitetaan ainoastaan kirjalliseen pyyntöön perustuen Suomen lain sallimissa ja velvoittamissa rajoissa ja Soneran yritysturvallisuusyksikön valvonnassa.

Varmenteen haltijalle luovutetaan häntä itseään koskevia arkistotietoja. Tiedot luovutetaan henkilötietolaissa määritellyn tarkastusoikeuden rajoissa veloituksetta. Muutoin tiedon hakemisesta ja toimittamisesta veloitetaan kohtuulliset työmäärään perustuvat maksut.

TeliaSonera Finland Oyj

Varmentaja huolehtii siitä, että sen arkistoista kulloinkin tarvittavat tiedot ovat haettavissa ja tarkistettavissa koko arkiston säilytyksen ajan.

4.8 Varmentajan allekirjoitusavaimen vaihtaminen

Varmentajalle luodaan uusi allekirjoitusavain ennen kuin käytössä olevan (vanhan) allekirjoitusavaimen käyttöaika varmenteiden allekirjoittamiseen päättyy. Uutta allekirjoitusavainta varten Varmentajalle luodaan myös uusi nimi, joka näkyy Varmentajan myöntämien varmenteiden ”Issuer”-kentässä.

Avainta käytetään varmenteiden allekirjoittamiseen korkeintaan niin kauan, että sillä myönnetyn viimeisenkin varmenteen voimassaoloaika on päättynyt, ennen kuin avaimen käyttöaika päättyy. Näin varmistetaan, että sulkulista voidaan aina allekirjoittaa samalla avaimella, jolla sille mahdollisesti päätyvät varmenteet on allekirjoitettu.

Seuraavat varmenteet julkaistaan avainten vaihtamisen yhteydessä:

- Varmentajan uudella yksityisellä avaimella allekirjoitettu varmenne Varmentajan vanhalle julkiselle avaimelle
- Varmentajan vanhalla yksityisellä avaimella allekirjoitettu varmenne Varmentajan uudelle julkiselle avaimelle
- Varmentajan uudella yksityisellä avaimella allekirjoitettu varmenne saman avainparin julkiselle avaimelle

4.9 Toipuminen katastrofeista ja avainten paljastumisesta

4.9.1 Toipuminen hätätilanteista

Poikkeus- ja vaaratilanteissa Varmentaja noudattaa jatkuvuussuunnitelmassa määriteltyä prosessia ja kyseisen tilanteen varalta mahdollisesti laadittua muuta ohjeistusta. Vaaratilanteissa varmenteiden myöntäminen keskeytetään ja tietoliikenneyhteydet Varmentajan tuotantojärjestelmiin katkaistaan, kunnes tilanne on palautunut normaaliksi.

4.9.2 Tietokoneresurssit, ohjelmisto ja/tai tieto ovat käyttökelvottomia

Tuotantojärjestelmä on kahdennettu. Laitevian tapauksessa tuotanto siirtyy varalaitteelle. Ohjelmistovian tapauksessa suoritetaan ohjelmiston uudelleenasennus. Tiedon korruptoituessa tiedot palautetaan varmuuskopiolta. Kriittisimmistä tiedoista otetaan varmuuskopio vähintään 4 kertaa viikossa. Laaja-alaisempi tuotantojärjestelmän osan tuhoutuminen aiheuttaa palvelun keskeytymisen, jonka pituus riippuu ongelman laajuudesta.

4.9.3 Varmentajan yksityisen avaimen paljastuminen

Mikäli Varmentajan yksityinen avain paljastuu, noudatetaan Varmentajan määrittelemää proseduuria. Avaimen käyttö lopetetaan välittömästi. Tällä avaimella allekirjoitetut sulkulistat poistetaan Sulkulistapalvelusta välittömästi, jolloin kyseisellä avaimella allekirjoitettuihin varmenteisiin ei voi riittävin perustein luottaa. Varmentaja ilmoittaa avaimen paljastumisesta sekä sen edellyttämistä toimenpiteistä sähköpostilla tai kirjeitse asiakasorganisaatioille sekä muille varmentajille, joiden kanssa sillä on sopimus. Toiminnan jatkaminen kyseisen varmenneluokan osalta vaatii uusien Varmentajan allekirjoitusavainten luonnin sekä uusien varmenteiden luonnin Varmenteen haltijoille.

4.9.4 Luonnon- tai muun katastrofin jälkeinen tuotantotilojen turvaaminen

Varmentajan tuotantotilat on rakennettu turvallisiksi ottaen huomioon tilojen maantieteellisen sijainnin mukaiset todennäköiset riskit.

4.10 Varmentajan toiminnan lopettaminen

Varmentajan toiminnan lopettaminen on tilanne, jossa varmenteiden myöntäminen lakkaa pysyvästi. Varmentajan allekirjoitusavainten vaihtamista tai varmennustoiminnan siirtämistä vastuineen toiselle organisaatiolle ei katsota Varmentajan toiminnan lopettamiseksi.

Toiminnan lopettamiseen liittyvät keskeiset toimenpiteet on kuvattu varmennepolitiikassa. Varmentajan Varmennepolitiikkayksikkö vastaa politiikan toteuttamisesta tältä osin.

Varmentaja tiedottaa toimintansa lopettamisesta seuraavasti:

- Tilaajille ja/tai asiakasorganisaatioille sekä muille varmentajille, joiden kanssa sillä on sopimus, kirjallisesti asiakkaan yhteysosoitteeseen,
- Rekisteröijille ja Varmenteen valmistajille ja muille alihankkijoille kirjeellä, jolla samalla irtisanotaan sopimus varmennepalveluiden toimintojen hoitamisesta Varmentajan puolesta.

Lisäksi Varmentaja toteuttaa seuraavat toimenpiteet toimintansa lopettamisen yhteydessä:

- Varmentaja peruuttaa alihankkijoiltaan varmennustoimintaan liittyvät valtuutukset ja pääsyoikeudet Varmentajan järjestelmiin.
- Varmentaja lopettaa Sulkulistapalvelun, jonka jälkeen sen myöntämiin varmenteisiin ei voi enää perustellusti luottaa.
- Varmentaja tuhoaa tai poistaa käytöstä yksityiset allekirjoitusavaimensa siten, että niitä ei voida enää ottaa käyttöön.

TeliaSonera Finland Oyj

5 Fyysisen turvallisuuden, käyttöturvallisuuden ja henkilöstöturvallisuuden hallinta

5.1 Fyysinen ja ympäristöön liittyvä tietoturvallisuus

Fyysisen turvallisuusvalvonnan avulla kontrolloidaan pääsyä Varmentajan ohjelmistoihin ja laitteistoihin. Näihin sisältyvät varmennusjärjestelmän työasemat sekä erilliset salaustekniset laitteet ja salaustekniset välineet. Kulunvalvontajärjestelmä kirjaa Varmentajan tiloihin saapumiset ja niistä lähtemiset.

Avaimet, joilla allekirjoitetaan varmenteita ja sulkulistoja suojataan fyysisesti siten, että ne eivät koskaan voi paljastua fyysisen hyökkäyksen tuloksena.

Varmentajan tiloihin on varastoitu varmuuskopiot ja tietovälineet siten, että tallennetun tiedon häviäminen, peukalointi tai luvaton käyttö on riittävällä varmuudella estetty. Varmuuskopioita säilytetään sekä tiedon palautuksia varten että tärkeän tiedon arkistoimiseksi.

Tietoturvapolitiikassa kuvattujen fyysisen turvallisuuden periaatteiden toteuttamiseksi Varmentaja ylläpitää kuvauksia tuotantojärjestelmän fyysisen turvallisuuden hallinnasta.

5.1.1 Tilojen sijainti ja rakenteet

Varmentajan turvallinen laitteisto sijaitsee Suomessa sellaisissa tiloissa, joiden fyysinen suojaus vastaa vähintään Viestintäviraston määräyksen viestintäverkon fyysisestä suojaamisesta (Viestintävirasto 48 B/2004 M) vaatimuksia ”erittäin tärkeille tiloille”.

5.1.2 Pääsy tiloihin

Varmenteiden tuotantotila on ympärivuorokautisen vartioinnin ja valvonnan piirissä. Pääsy tilaan, jossa varmennusjärjestelmä sijaitsee on rajattu tietyille Varmentajan luotetuissa rooleissa toimiville henkilöille. Pääsy laitteistoon, jossa Varmentajan allekirjoitusavaimet sijaitsevat ja jossa niiden käyttö on mahdollista, vaatii kahden sellaisen henkilön läsnäoloa, joille on erikseen annettu oikeus saapua alueelle.

Pääsy muihin tiloihin, joissa sijaitsee osia varmennusjärjestelmästä, on rajoitettu niihin henkilöihin, jotka toimivat jossakin kappaleessa 5.2.1 ”Luotetut roolit” mainituista rooleista. Pääsyä tiloihin valvotaan kulunvalvontajärjestelmällä. Mikäli henkilölle ei ole myönnetty pysyvää henkilökohtaista kulkuoikeutta, hän voi liikkua tiloissa ainoastaan jonkun kulkuun oikeutetun henkilön seurassa.

Rekisteröintipisteiden tulee sijaita tiloissa, joihin pääsyä voidaan valvoa. Varmentajan omissa ja Varmentajan valtuuttamien Rekisteröijien rekisteröintipisteissä, joihin yleisöllä on pääsy, noudatetaan näiden pisteiden valvonnasta annettuja ohjeita.

5.1.3 Virransyöttö ja ilmastointi

Varmennusjärjestelmän keskeytymätön toiminta varmistetaan katkeamattoman virransyöttöjärjestelmän ja varavoimalaitteiden avulla. Laitetiloissa on ilmastointijärjestelmä, jonka tuottaman ilman lämpötilaa ja kosteutta monitoroidaan jatkuvasti.

TeliaSonera Finland Oyj

5.1.4 Vesivahingoille altistuminen

Rakenteellisilla ratkaisuilla estetään vesivahingoille altistuminen. Laitetilaa valvotaan kosteusilmaisimilla.

5.1.5 Palontorjunta

Laitetilat kuuluvat automaattisen palohälytysjärjestelmän piiriin. Tilat on varustettu savunilmaisimilla ja käsisammuttimilla.

5.1.6 Tallenteet

Tietovälineet, joille on tallennettu Varmentajan tuotantojärjestelmään liittyvää tai siinä syntyvää tietoa, varastoidaan samoissa turvallisissa tiloissa, joissa itse järjestelmä sijaitsee. Ks. myös kappale 5.1.8 ”Varmuuskopioiden tallennus erillään”.

5.1.7 Jätemateriaalin käsittely

Varmennusjärjestelmän levyt, magneettinauhat ja asennuslevykkeet varmuuskopioineen, joita ei varastoida pysyvästi Varmentajan tuotantotiloihin, hävitetään turvallisesti niiden tultua tarpeettomiksi.

5.1.8 Varmuuskopioiden tallennus erillään

Varmennusjärjestelmän tuottamista lokitiedoista otetaan varmuuskopiot, jotka säilytetään Varmentajan tuotantotiloista erillään sijaitsevissa tiloissa. Pääsy näihin tiloihin on rajoitettu erikseen valtuutetuille henkilöille kuin pääsy varmenteiden tuotantotiloihin.

5.2 Käyttöturvallisuus

5.2.1 Luotetut roolit

Varmennustoimintaan osallistuva henkilöstö on jaoteltu seuraaviin luotettuihin rooleihin, joiden vastuut on kuvattu varmennepolitiikoissa:

Tietoturvallisuusvastaava (Security Manager)
Järjestelmän pääkäyttäjä (PKI Administrator)
Järjestelmän ylläpitäjä (System Administrator)
Rekisteröintivastaava (Registration Officer)
Sulkupalveluvastaava (Revocation Officer)

Luotetuissa rooleissa toimivat henkilöt sitoutuvat noudattamaan tätä varmennuskäytäntöä.

5.2.2 Tehtäviin tarvittavien henkilöiden lukumäärä

Varmentaja huolehtii siitä että jokaista tehtävää kohden on palkattu riittävästi henkilöstöä ja että yksittäiset henkilöt eivät voi toimia kaikissa rooleissa samanaikaisesti.

Tiettyihin toimenpiteisiin vaaditaan usean henkilön yhtäaikainen osallistuminen. Varmenteiden tuotantoon kohdistuvien kriittisten toimenpiteiden toteuttaminen tuotantotiloissa vaatii vähintään kahden henkilön osallistumisen. Varmentajan määrittelemien proseduurien mukaisesti tehtävä Varmentajan yksityisen avaimen luonti sekä Varmentajan yksityisen avaimen varmuuskopiointi ja palauttaminen edellyttävät vähintään kahden henkilön paikallaoloa.

5.2.3 Rooleihin liittyvä tunnistaminen

Seuraavissa rooleissa toimivien tunnistamiseen vaaditaan varmenne:

Järjestelmän pääkäyttäjä
Rekisteröintivastaava *
Sulkupalveluvastaava

* SoneraClass 2 –varmenteiden rekisteröinnissä voidaan käyttää myös muuta vahvaa tunnistustapaa Rekisteröintivastaavan tunnistamiseksi (eg. one-time SMS password).

Alla luetelluissa rooleissa tunnistamisessa käytetään pääsääntöisesti käyttäjätunnusta ja salasanaa. Silloin kun rooliin kuuluvien velvollisuuksien hoitaminen edellyttää Varmentajan kriittisimpien järjestelmien käyttöä, kirjautuminen näihin edellyttää myös alla luetelluissa rooleissa toimivilta varmenteeseen tai kertakäyttösalasanaan pohjautuvaa tunnistamista.

Tietoturvallisuusvastaava
Järjestelmän ylläpitäjä

5.2.4 Sisäinen dokumentaatio

Kappaleessa 2.7.1 ”Varmentajan tiedot ja tietovarastot” lueteltujen julkisten dokumenttien lisäksi Varmentaja ylläpitää ja kehittää jatkuvasti sisäistä dokumentaatiota organisaatiossaan työskentelevien henkilöiden käyttöön. Tähän dokumentaatioon kuuluu ainakin:

- tietoturvapolitiikka
- järjestelmän tekniset kuvaukset
- kuvaus varmennustoimintaan osallistuvasta organisaatiosta
- Varmentajan organisaatioon kuuluviin rooleihin liittyvät työnkuvaukset
- työohjeet
- prosessikuvaukset
- jatkuvuussuunnitelma

5.3 Henkilöstöturvallisuus

5.3.1 Taustatiedot, pätevyys, työkokemus ja muut vaatimukset

Varmentajan työntekijöiden palkkaamisessa noudatetaan Soneran normaaleja työhönottomenettelyjä työhönottotarkastuksineen. Varmentaja huolehtii siitä, että jokaisella sen varmennustoimintaan liittyviin tehtäviin palkkaamalla henkilöllä on tarvittava pätevyys ja kokemus tehtäviensä suorittamiseen. Alihankkijat, joiden työntekijöitä toimii Varmentajan tärkeissä rooleissa, velvoitetaan sopimuksella huolehtimaan tästä omien työntekijöidensä osalta.

Sonera on määritellyt ja ylläpitää kattavia yritysturvallisuuteen liittyviä ohjeistoja (politiikat, standardit, toimintaohjeet, määräykset ja säädökset), jotka jokaisen työntekijän on tiedettävä ja tunnettava.

Jokainen Varmentajan omaan organisaatioon kuuluva työntekijä, jonka työtehtäviin kuuluu varmennustoimintaan liittyviä tehtäviä, allekirjoittaa henkilökohtaisen salassapitosopimuksen. Myös jokainen

Varmenteen valmistaja tai muu Varmentajan alihankkija, jonka työntekijöitä toimii Varmentajan luotetuissa rooleissa, allekirjoittaa salassapitosopimuksen, joka velvoittaa sen työntekijöitä.

5.3.2 Taustatietojen tarkistaminen

Kaikkien Varmentajan työtehtäviin palkattavien henkilöiden taustatietojen tarkistuksessa noudatetaan Soneran märittelemiä työhönottomenettelyjä työhönottotarkastuksineen.

Seuraavissa rooleissa toimiville henkilöille suoritetaan kolmannen osapuolen toimesta taustatietojen tarkistaminen:

Tietoturvallisuusvastaava
Järjestelmän pääkäyttäjä
Varmentajan Rekisteröintivastaava

Muutoin Varmentaja tarkistuttaa työntekijöidensä taustatiedot harkintansa mukaan riippuen työntekijän roolista Varmentajan organisaatiossa. Tarkistuttaminen uusitaan tarvittaessa Varmentajan harkinnan mukaan. Varmentaja velvoittaa sopimuksin alihankkijansa huolehtimaan tärkeissä rooleissa toimivien työntekijöidensä taustatietojen tarkistuttamisesta.

5.3.3 Koulutusvaatimukset

Varmentajan uudet työntekijät perehdytetään varmennustoimintaan yleisesti, siihen liittyviin turvallisuusvaatimuksiin sekä erityisesti omiin työtehtäviinsä. Käsiteltävään aineistoon kuuluu mm. tietoturvapolitiikka, varmennepolitiikka ja varmennuskäytäntö. Tarvittaessa järjestetään henkilön työtehtäviin ja rooliin sovitettu yksilöllinen perehdyttäminen ja koulutus.

Varmentajan työntekijöille järjestetään tarvittaessa täydennyskoulutusta.

Vastuu alihankkijoiden työntekijöiden koulutuksesta on alihankkijoilla itsellään sopimuksiin perustuen.

5.3.4 Seuraukset luvattomista toimenpiteistä

Jos Varmentaja havaitsee väärinkäytöksen, siihen syyllistynyt Varmentajan työntekijä siirretään välittömästi toisiin tehtäviin ja kaikki hänen pääsyoikeutensa varmennustoimintaan liittyviin järjestelmiin peruutetaan. Jatkotoimenpiteiden suhteen noudatetaan Soneran voimassa olevia käytäntöjä.

Väärinkäytöstilanteissa alihankkijoiden tapauksessa noudatetaan sopimuksissa määriteltyjä menettelyjä.

5.3.5 Henkilöstölle toimitettava dokumentaatio

Jokaiselle varmennustoimintaan liittyvään tehtävään palkattavalle Varmentajan työntekijälle annetaan pääsy varmennustoimintaan ja Varmentajan toimintaan liittyvään dokumentaatioon. Lisäksi työntekijöille annetaan erityisesti heidän omien työtehtäviensä suorittamiseen tarvittavat ohjeet ja muu materiaali. Ohjeistusta on saatavilla myös suoraan sähköisessä muodossa työntekijöiden käytössä olevien järjestelmien ja sovellusten käytön yhteydessä.

Varmentaja toimittaa alihankkijoille näiden tarvitseman perusdokumentaation, jonka toimittamisesta työntekijöilleen alihankkija vastaa. Tiettyjen alihankkijoiden työntekijöillä on heidän käyttämiensä sovellusten kautta pääsy Varmentajan ylläpitämiin ohjeisiin. Varmentaja toimittaa dokumentaatiota myös henkilökohtaisesti tietyissä rooleissa toimiville alihankkijoiden työntekijöille. Lisäksi alihankkijat velvoitetaan toimittamaan muu tarvittava dokumentaatio työntekijöilleen.

6 Teknisen turvallisuuden hallinta

Tämä luku sisältää julkisten ja yksityisten avainten hallintapolitiikan ja siihen liittyvän teknisen valvonnan vaatimukset, jotka koskevat Varmentajaa, Rekisteröijiä, Varmenteen valmistajia ja Varmenteen haltijoita.

Varmenteen haltijoiden avainparit luo toimikorteille ja Varmenne-SIM -korteille Varmentajan tähän tarkoitukseen hyväksymä Varmenteen valmistaja, Korttivalmistaja. USB-avaimelle voi Varmenteen haltijan avainparin luoda Varmentajan organisaatioon kuuluva Rekisteröijä tai Rekisteröijänä toimiva asiakasorganisaatio. Ohjelmistovarmenteeseen liittyvän avainparin luo Varmentajan organisaatioon kuuluva Rekisteröijä, asiakasorganisaatiossa toimiva Rekisteröintivastaava tai Varmenteen hakija itse.

Varmentajan, Varmenteen valmistajien, Rekisteröijien ja Varmenteen haltijoiden avainparit luodaan ja toimitetaan niiden valtuutetuille käyttäjille siten, että yksityiseen avaimeen ei pääse käsiksi kukaan muu kuin käyttäjä.

6.1 Varmentajan avainparin luonti, käyttöönotto ja suojaaminen

6.1.1 Varmentajan avainparin luonti

Varmentajan avainparin luonti tapahtuu Varmentajan määrittelemän avaintenluontiproseduurin mukaisesti. Avainpari luodaan Varmentajan fyysisesti suojatuissa tiloissa varmennusjärjestelmää hyväksi käyttäen salausteknisessä laitteessa (ks. kappale 6.1.6 ”Varmentajan yksityisen avaimen suojaaminen”). Avaintenluontiin osallistuvat henkilöt ovat luotetuissa rooleissa toimivia Varmentajan tähän tehtävään valtuuttamia henkilöitä, joista vähintään kahden on oltava paikalla. Avaintenluontiproseduurin toimenpiteet kirjataan pöytäkirjaan, ja jokainen proseduuriin osallistuva henkilö vahvistaa pöytäkirjan allekirjoituksellaan. Pöytäkirja säilytetään kappaleen 4.7 ”Tietojen arkistointi” mukaisesti.

6.1.2 Varmentajan julkisen avaimen toimittaminen käyttäjille

Varmentajan julkinen avain on saatavilla internetistä osoitteesta http://support.partnergate.sonera.com/, jossa julkaistaan Varmentajan itsensä allekirjoittama Varmentajan julkisen avaimen varmenne sekä varmenteen tiiviste, ns. sormenjälki.

6.1.3 Varmentajan avainten pituudet ja käytetty algoritmi

Varmentaja käyttää varmenteiden ja sulkulistatietojen allekirjoittamiseen RSA-algoritmiin perustuvaa allekirjoitusavainta, jonka pituus on vähintään 2048 bittiä.

6.1.4 Varmentajan avainparin käyttöikä

Varmentajan yksityisen avaimen käyttöikä on korkeintaan kaksikymmentäviisi (25) vuotta. Käyttöikä ei voi olla pidempi kuin avaimeen liittyvän Varmentajan varmenteen voimassaoloaika. Mikäli Varmenteen haltijan varmenne peruutetaan, sulkulista allekirjoitetaan samalla avaimella, jolla kyseinen varmenne on allekirjoitettu. Avainta on voitava käyttää siihen liittyvän varmenteen voimassaoloaikana viimeisenkin sillä allekirjoitetun Varmenteen haltijan varmenteen peruuttamiseen koko tämän varmenteen voimassaoloajan. Avainta voidaan siis käyttää Varmenteen haltijoiden varmenteiden allekirjoittamiseen avaimen käyttöiän ajan vähennettynä

Varmenteen haltijan varmenteen voimassaoloajalla. Tämän jälkeen Varmentajalle tulee luoda uusi avainpari varmenteiden allekirjoitukseen.

6.1.5 Varmentajan avainten käyttötarkoitukset

Varmentajan allekirjoitusavaimia voidaan käyttää vain Varmentajan fyysisesti suojatuissa tiloissa Varmentajan luotetuissa rooleissa toimivien henkilöiden valvonnassa käyttäen varmennusjärjestelmää ja kappaleessa 6.1.6 ”Varmentajan yksityisen avaimen suojaaminen” määriteltyä salausteknistä laitetta.

Varmentajan julkisen avaimen käyttötarkoitukset, jotka on ilmoitettu Varmentajan varmenteen “key usage”-kentässä, ovat:

- keyCertSign (Varmentajan allekirjoituksen tarkistaminen Varmenteen haltijoiden varmenteista)
- CRLSign (Varmentajan julkaisemien sulkulistatietojen allekirjoituksen tarkistaminen).

6.1.6 Varmentajan yksityisen avaimen suojaaminen

Varmentaja on toteuttanut yksityisen allekirjoitusavaimensa suojaamisen fyysisten suojausten, määriteltyjen proseduurien, pääsynvalvonnan ja käyttöoikeuksien yhdistelmällä.

Varmentajan turvallisissa fyysisesti suojatuissa tiloissa sijaitsevaan varmennusjärjestelmään kuuluu salaustekninen laite, jolla Varmentajan allekirjoitusavain on suojattu. Salaustekninen laite noudattaa vähintään FIPS 140-2 level 3 -standardia.

Varmentaja huolehtii teknisen valvonnan ja määriteltyjen proseduurien avulla, että kukaan ei yksinään saa haltuunsa keinoja siihen ympäristöön pääsemiseksi, jossa yksityinen avain on tallennettuna, tai pysty käyttämään avainta millään tavalla. Kriittisiä allekirjoitusavaimeen liittyviä toimenpiteitä, kuten avaimen tallennus, varmistus ja palautus, on suorittamassa aina useampi kuin yksi henkilö.

Avaimen palautus edellyttää sellaisen aktivointitiedon käyttöä, joka on tallennettu osiin jaettuna erillisiin turvallisiin tiloihin ja jonka haltuun saanti on hajautettu Varmentajan määrittelemälle määrälle luotetuissa rooleissa toimivia henkilöitä. Avaimen palauttaminen edellyttää, että tietty määrä näistä henkilöistä osallistuu palautusproseduuriin.

6.1.7 Varmentajan yksityisen avaimen key escrow

Varmentajan yksityiselle avaimelle ei suoriteta key escrow –tyyppistä kopiointia ja tallennusta missään olosuhteissa.

6.1.8 Varmentajan yksityisen avaimen varmuuskopiointi

Varmentajan yksityisen allekirjoitusavaimen tuhoutumisen varalta on olemassa järjestely sen palauttamiseksi. Varmentajan yksityisen avaimen varmuuskopiointi on hoidettu tavalla, joka takaa kaikissa tilanteissa vähintään saman turvatason, mitä vaaditaan varmennusjärjestelmässä käytössä olevien yksityisten avainten ylläpidolta (ks. kappale 6.1.6 ”Varmentajan yksityisen avaimen suojaaminen”).

6.1.9 Varmentajan yksityisen avaimen arkistointi

Varmentajan yksityisiä avaimia ei arkistoida.

TeliaSonera Finland Oyj

6.1.10 Varmentajan yksityisen avaimen aktivointi

Varmentajan yksityisen avaimen aktivointi sisältyy kappaleen 6.1.1 ”Varmentajan avainparin luonti” mukaiseen proseduuriin. Aktivointiin vaaditaan vähintään yksi Varmentajan luotetussa roolissa toimiva henkilö, jonka varmennusjärjestelmä tunnistaa vahvalla tunnistamismekanismilla. Avain säilyy varmennusjärjestelmässä aktiivisena, kunnes sen käyttö keskeytetään esim. huoltotoimenpiteiden takia.

6.1.11 Varmentajan yksityisen avaimen deaktivointi

Varmentajan yksityisen avaimen deaktivointiin vaaditaan vähintään yksi Varmentajan luotetussa roolissa toimiva henkilö.

6.1.12 Varmentajan yksityisen avaimen tuhoaminen

Kun Varmentajan yksityisen avaimen käyttö lopetetaan, sen kaikki kopiot tuhotaan tai niitä säilytetään siten, että niiden käyttö on estetty.

6.1.13 Varmentajan julkisen avaimen arkistointi

Varmentaja arkistoi voimassa olevat ja vanhentuneet Varmentajan julkiset avaimet kappaleen 4.7 ”Tietojen arkistointi” mukaisesti.

6.2 Varmenteen haltijan avainparin luonti, käyttöönotto ja suojaus

6.2.1 Varmenteen haltijan avainparin luonti

Class 1
Varmentajan alihankkijana toimiva Korttivalmistaja huolehtii turvallisesta Varmenteen haltijoiden avainparien luonnista toimikorteille. Korttivalmistajan avaintenluontijärjestelmän tuottamat avainparit ovat yksilöllisiä ja ne luodaan joko kortin sisällä tai erillisessä järjestelmässä. Kortille voidaan luoda useampia avaimia. Sähköisen allekirjoituksen kiistämättömyyden todentaminen käytettävä avainpari luodaan siten, että yksityinen avain tallennetaan ainoastaan kortille eikä siitä jää kopiota avaintenluontijärjestelmään. Sähköisessä muodossa olevan tiedon luottamuksellisuuden varmistamiseen käytettävästä yksityisestä avaimesta voidaan ottaa varmuuskopio, mikäli asiasta on Tilaajan kanssa sopimuksella sovittu.

Avainpari voidaan luoda asiakasorganisaatiossa USB-avaimelle. Tällöin asiakasorganisaatio on itse vastuussa avainparin turvallisesta luomisesta ja yksityisen avaimen luottamuksellisuuden säilymisestä.

Jos avainpari luodaan USB-avaimelle Varmentajan toimesta, luominen tapahtuu Varmentajan määrittelemien turvallisten menettelyjen mukaisesti USB-avaimen sisällä eikä yksityisestä avaimesta synny kopiota.

Class 2
Avainparit luodaan asiakasorganisaatiossa selain- tai palvelinohjelmiston avulla. Tällöin asiakasorganisaatio on itse vastuussa avainparin turvallisesta luomisesta ja yksityisen avaimen luottamuksellisuuden säilymisestä.

Jos avainpari luodaan Varmentajan toimesta, luominen tapahtuu Varmentajan määrittelemien turvallisten menettelyjen mukaisesti.

Mobiilivarmenne
Varmentajan alihankkijana toimiva Korttivalmistaja huolehtii turvallisesta Varmenteen haltijoiden avainparien luonnista Varmenne-SIM -korteille. Korttivalmistajan avaintenluontijärjestelmän tuottamat avainparit ovat yksilöllisiä ja ne luodaan joko kortin sisällä tai erillisessä järjestelmässä. Avainpari luodaan siten, että yksityinen avain tallennetaan ainoastaan kortille eikä siitä jää kopiota avaintenluontijärjestelmään. Kortille voidaan luoda useampia avaimia.

6.2.2 Varmenteen haltijan yksityisen avaimen toimittaminen Varmenteen haltijalle

Varmentaja toimittaa Varmenteen haltijan yksityisen avaimen tälle toimikortilla, USB-avaimella, tiedostossa tai Varmenne-SIM -kortilla. Varmentaja tilaa allekirjoituksen luomisvälineitä vain tunnetuilta toimittajilta.

Toimikortit
Korttivalmistaja toimittaa yksityiset avaimet sisältävät toimikortit korttitilauksessa määriteltyyn osoitteeseen, joka voi olla asiakasorganisaation Rekisteröintivastaavan osoite tai suoraan Varmenteen haltijan osoite. Rekisteröintivastaava toimittaa kortin Varmenteen haltijalle varmistuttuaan tämän henkilöllisyydestä.

USB-avaimet
Jos avainparit luodaan Varmentajan rekisteröintipisteessä, USB-avaimet toimitetaan kirjattuna kirjeenä asiakasorganisaation rekisteröintipisteeseen. Rekisteröintipisteessä USB-avain luovutetaan Varmenteen haltijalle tämän henkilöllisyyden varmistamisen jälkeen.

Ohjelmistovarmenteet
Kun Varmenteen hakija luo avainparinsa itse, yksityinen avain tallentuu hänen työasemalleen, jolloin erillistä avaimen toimitusta ei tarvita. Jos asiakasorganisaation Rekisteröintivastaava luo avainparin, yksityisen avaimen toimitus Varmenteen haltijalle on asiakasorganisaation vastuulla. Jos Varmentaja luo avainparin, Varmentaja toimittaa yksityisen avaimen tiedostossa sähköpostin välityksellä Varmenteen haltijalle. Tiedostosta jää virhetilanteiden varalta Varmentajalle korkeintaan viiden arkipäivän ajaksi kopio, joka toimitetaan tarvittaessa Varmenteen haltijalle. Kun on kyseessä Soneran tietoturvapalvelun vaatima palvelimen käyttämä laitevarmenne, jonka hakee Varmentajan henkilöstö, yksityinen avain tallentuu laitteelle varmennetta haettaessa.

Varmenne-SIM -kortit
Korttivalmistaja toimittaa yksityiset avaimet sisältävät Varmenne-SIM -kortit Varmentajan määrittelemän turvallisen prosessin mukaisesti Varmentajan nimeämään varastopisteeseen. Tästä pisteestä kortit toimitetaan valtuutettujen Rekisteröijien tekemissä korttitilauksessa määriteltyihin rekisteröintipisteiden osoitteisiin. Varmenteen haltijalle annetaan Varmenne-SIM -kortti rekisteröintipisteessä.

6.2.3 Varmenteen haltijan julkisen avaimen toimittaminen Varmentajalle

Pääsääntöisesti julkinen avain toimitetaan sähköisesti allekirjoitettuna ja salattua yhteyttä käyttäen varmennusjärjestelmään suoraan siitä pisteestä, jossa avaimet on luotu. Poikkeukset tähän sääntöön on kuvattu asianomaisissa varmennepolitiikoissa.

6.2.4 Varmenteen haltijan avainten pituudet ja käytetty algoritmi

Class 1 ja Mobiilivarmenne
Varmenteen haltijoiden käytössä olevien RSA-algoritmin yhteydessä käytettävien avainten pituus on vähintään 1024 bittiä.

Class 2
Varmenteen haltijoiden käytössä olevien RSA-algoritmin yhteydessä käytettävien avainten pituus on

pääsääntöisesti 1024 bittiä. Varmenteen haltijan käytössä oleva selainohjelmiston versio saattaa rajoittaa avaimen pituutta.

6.2.5 Varmenteen haltijan avainparin käyttöikä

Varmenteen haltijan avainten käyttöikä on ilmoitettu asianomaisen varmenneluokan varmennepolitiikassa.

6.2.6 Varmenteen haltijan avainten käyttötarkoitukset

Varmenteen haltijan yksityisiä avaimia voidaan käyttää ainoastaan sellaisiin tarkoituksiin, jotka vastaavat kappaleen 7.1.1.3 ”Varmenteen kenttien sisällöt” taulukoissa mainittuja eri varmenneluokkiin liittyvien julkisten avainten käyttötarkoituksia.

6.2.7 Varmenteen haltijan yksityisen avaimen suojaaminen

Kun Varmentaja luo avaimet, niiden toimitus Tilaajalle tai Varmenteen haltijalle tapahtuu Varmentajan määrittelemän prosessin mukaisesti (ks. kappale 6.2.2 ”Varmenteen haltijan yksityisen avaimen toimittaminen Varmenteen haltijalle”). Kun Varmentaja luo ohjelmistovarmenteeseen liittyvät avaimet, Varmentaja säilyttää korkeintaan viiden arkipäivän ajan kopiota tiedostosta, joka sisältää yksityisen avaimen.

Asiakasorganisaatiolla ja sen Rekisteröintivastaavilla ja käyttäjillä on velvollisuus noudattaa avainten suojauksessa Varmentajan antamia ohjeita, jotka sisältyvät dokumenttiin ”Soneran varmennepalvelut, Asiakkaan vastuut”.

Class 1
Yksityiset avaimet on tallennettu ISO 7816 –standardin mukaiselle toimikortille tai USB-avaimelle.

Class 2
Yksityiset avaimet on tallennettu työaseman tai palvelimen ohjelmistoon.

Mobiilivarmenne
Yksityiset avaimet on tallennettu Varmenne-SIM -kortille, joka on ISO 7816 –standardin sekä ETSI:n standardien TS GSM 11.11 ja 11.14 sekä 03.48 mukainen.

6.2.8 Varmenteen haltijan yksityisen avaimen key escrow

Varmenteen haltijan yksityiselle avaimelle ei suoriteta key escrow –tyyppistä kopiointia ja tallennusta missään olosuhteissa.

6.2.9 Varmenteen haltijan yksityisen avaimen varmuuskopiointi

Varmentaja ei ota Varmenteen haltijan yksityisestä avaimesta varmuuskopioita lukuun ottamatta seuraavia tilanteita:

- Kun Varmentaja luo Varmenteen haltijan ohjelmistovarmenteeseen liittyvän yksityisen avaimen, Varmentaja säilyttää kopiota avaimen sisältävästä tiedostosta virhetilanteiden varalta 5 arkipäivän ajan.
- Asiakasorganisaation kanssa voidaan erikseen sopia, että Varmentaja ottaa varmuuskopion toimikortille tallennettavasta sähköisessä muodossa olevan tiedon luottamuksellisuuden varmistamiseen käytettävästä yksityisestä avaimesta.

6.2.10 Varmenteen haltijan yksityisen avaimen arkistointi

Varmenteen haltijan yksityistä avainta ei arkistoida ellei siitä erikseen sovita asiakkaan kanssa..

6.2.11 Varmenteen haltijan yksityisen avaimen aktivointi

Class 1 ja Mobiilivarmenne
Varmenteen haltijan yksityinen avain vaatii aktivoinnin tunnusluvulla.

Class 2
Asiakasorganisaatioille suositellaan PIN-koodin käyttöä yksityisen avaimen aktivoinnissa dokumentin ”Soneran varmennepalvelut, Asiakkaan vastuut” kuvaamalla tavalla.

6.2.12 Varmenteen haltijan yksityisen avaimen lukkiutuminen

Class 1
Toimikortilla oleva yksityinen avain lukkiutuu, jos siihen liittyvä tunnusluku syötetään väärin viisi (5) kertaa peräkkäin. Lukkiutunut avain voidaan palauttaa käyttöön PUK-koodin avulla (PUK = PIN Unblocking Key). Asiakasorganisaatio voi päättää käyttäjiensä osalta hyödynnetäänkö PUK-toiminnetta. PUK-koodilistaa ylläpitää Varmentaja, tai asiakasorganisaation rekisteröintipiste omien käyttäjiensä osalta, tai Varmenteen haltija säilyttää itse saamansa PUK-koodin.

USB-avaimissa ei oletusarvoisesti ole käytössä PUK-koodia, ja yksityinen avain lukkiutuu, jos siihen liittyvä tunnusluku syötetään väärin viisitoista (15) kertaa peräkkäin. Asiakasorganisaation rekisteröintipisteessä, jossa luodaan avainpari USB-avaimelle, näitä oletusarvoja voidaan muuttaa. Asiakasorganisaation Rekisteröintivastaava voi organisaation oman päätöksen mukaisesti muuttaa lukkiutumiseen johtavaa väärin syötettyjen tunnuslukujen määrää sekä ottaa PUK-koodin käyttöön. PUK-koodien säilytyksen organisoi tällöin asiakasorganisaation rekisteröintipiste omien käyttäjiensä osalta.

Class 2
Varmenteen haltijan yksityisen avaimen lukkiutuminen riippuu käytössä olevasta ohjelmistosta.

Mobiilivarmenne
Yksityinen avain lukkiutuu, jos siihen liittyvä tunnusluku syötetään väärin viisi (5) kertaa peräkkäin. Lukkiutunutta avainta ei voi palauttaa käyttöön.

6.2.13 Varmenteen haltijan yksityisen avaimen tuhoaminen

Kun Varmenteen haltijan varmenne on vanhentunut eikä varmennetta ole uusittu, siihen liittyvää yksityistä avainta ei voi enää käyttää varmennepalveluiden yhteydessä. Avainta ei palauteta Varmentajalle tuhottavaksi, vaan se jää Varmenteen haltijan haltuun.

6.2.14 Varmenteen haltijan julkisen avaimen arkistointi

Varmentaja arkistoi Varmenteen haltijan julkisen avaimen kappaleen 4.7 ”Tietojen arkistointi” mukaisesti.

6.3 Varmenteen haltijan aktivointitieto

Varmenteen haltija käyttää yksityisiä avaimiaan tunnuslukujen avulla, jotka annetaan kortinlukijan, työaseman tai matkapuhelimen näppäimistöllä. Jokaista yksityistä avainta kohden on oma tunnuslukunsa. Tunnusluvun pituus riippuu varmennetyypistä ja avaimen käyttötarkoituksesta.

6.3.1 Aktivointitiedon luonti ja käyttöönotto

Kun Varmenteen haltijalla on mahdollisuus vaihtaa tunnusluku, Tilaajan velvollisuutena on huolehtia siitä että uusi tunnusluku koostuu riittävän monesta merkistä, eikä ole helposti arvattavissa tai pääteltävissä.

Class 1
Korttivalmistaja luo tunnusluvun samalla kun avainpari luodaan toimikortille. Tunnusluku annetaan Varmenteen haltijalle joko kortin luovuttamisen yhteydessä tai se lähetetään erikseen Varmenteen haltijan osoitteeseen.

Jos avainpari luodaan USB-avaimelle Varmentajan rekisteröintipisteessä, asiakasorganisaation Rekisteröintivastaavalle ilmoitetaan yksityisen avaimen käyttöön tarvittava vakioarvoinen PIN-koodi. Rekisteröintivastaavan tulee ohjeistaa Varmenteen haltijaa vaihtamaan PIN-koodi turvallisuussyistä ensimmäisellä käyttökerralla. Jos avainpari luodaan USB-avaimelle asiakasorganisaatiossa, organisaatio vastaa aktivointitiedon turvallisesta käyttöönotosta.

Class 2
Kun Varmenteen hakija luo avainparinsa itse, hän voi valita haluamansa PIN-koodin yksityisen avaimensa aktivointitiedoksi organisaationsa antamien ohjeiden mukaisesti. Jos asiakasorganisaation Rekisteröintivastaava tai Varmentaja luo avainparin, hän toimittaa yksityisen avaimen ja sen käyttöön tarvittavan PIN-koodin Varmenteen haltijalle erillisinä lähetyksinä.

Mobiilivarmenne
Korttivalmistaja luo tunnusluvun samalla kun avainpari luodaan Varmenne-SIM -kortille. Tunnusluku annetaan Varmenteen haltijalle rekisteröintipisteessä rekisteröinnin yhteydessä samalla kun hänelle luovutetaan Varmenne-SIM -kortti.

6.3.2 Aktivointitiedon suojaaminen

Silloin kun Korttivalmistaja luo avainparit, samassa yhteydessä luotavat tunnusluvut peitetään suojapinnalla tai suljetaan suojakuoreen, jota rikkomatta niitä ei pääse näkemään. Vastaanottaessaan tunnusluvut sisältävän kuoren Varmenteen haltijan tulee varmistaa, että suojapinta tai suojakuori on koskematon.

Silloin kun Varmentajan rekisteröintipiste luo avainparin, tunnusluku ja yksityinen avain toimitetaan Varmenteen haltijalle erillisinä lähetyksinä eri kanavia pitkin (poikkeuksena USB-avainten vakioarvoinen tunnusluku, ks. kappale 6.3.1 ”Aktivointitiedon luonti ja käyttöönotto”). Tunnusluku voidaan toimittaa esim. matkapuhelimeen SMS-viestinä tai antaa puhelimitse.

Silloin kun asiakasorganisaation Rekisteröintivastaava luo avainparit, tunnuslukujen turvallinen toimitus Varmenteen haltijalle on organisaation vastuulla.

Tilaajan tulee ohjeistaa Varmenteen haltijaa säilyttämään aktivointitietonsa riittävän turvallisesti. Tämän tulisi painaa aktivointitieto mieleensä. Aktivointitietoa ei saa paljastaa muille.

TeliaSonera Finland Oyj

6.4 Tietojärjestelmien turvavaatimukset

Tietojärjestelmien tietoturvan ylläpidossa noudatetaan Varmentajan tietoturvapolitiikan vaatimuksia.

6.4.1 Tietojärjestelmien turvaluokitus

Varmentajan järjestelmien turvaluokituksessa noudatetaan Soneran määrittelemää monitasoista tietojärjestelmien turvaluokituskäytäntöä.

6.4.2 Tietojärjestelmän käyttäjien tunnistaminen ja pääsynvalvonta

Pääsynvalvonnalla huolehditaan eri rooleissa toimivien järjestelmän käyttäjien tunnistamisesta ennen järjestelmään pääsyä (ks. kappale 5.2.3 ”Rooleihin liittyvä tunnistaminen”). Järjestelmä tarjoaa myös eri käyttäjien tekemien toimenpiteiden jäljitettävyyden.

6.4.3 Usean henkilön osallistumista vaativat toimenpiteet

Tiettyjen varmennusjärjestelmään liittyvien toimenpiteiden suorittaminen edellyttää usean henkilön osallistumista (ks. kappale 5.2.2 ”Tehtäviin tarvittavien henkilöiden lukumäärä”).

6.4.4 Kapasiteetin valvonta

Järjestelmän resurssien käyttö on jatkuvassa seurannassa ja automaattinen valvontajärjestelmä antaa hälytyksen asetettujen rajojen ylittyessä.

6.4.5 Tietoturvallisuuden valvontaan liittyvät vaatimukset

Varmentajan järjestelmien ja toiminnan tietoturvallisuuden valvontaan liittyvät vaatimukset on kuvattu kappaleessa 4.6 ”Tietoturvallisuuden valvonta”.

6.4.6 Poikkeustilanteiden hoito

Erilaisten poikkeustilanteiden varalta on määritelty raportointimenettelyt ja toimenpidesuunnitelmat. Varmentajan laatimassa liiketoiminnan jatkuvuussuunnitelmassa kuvataan toimenpiteet Varmentajan liiketoiminnan jatkuvuuden ollessa uhattuna.

6.4.7 Tietoaineistoon liittyvät turvavaatimukset

Tallenteiden varastointi, arkistointi ja tarpeettomaksi tulleen tietoaineiston käsittely on kuvattu kappaleissa 5.1.6 ”Tallenteet” ja 5.1.7 ”Jätemateriaalin käsittely”.

TeliaSonera Finland Oyj

6.5 Elinkaareen liittyvät tekniset turvatoimet

6.5.1 Järjestelmäkehityksen hallinta

Varmentajan tuotantojärjestelmän kehityksessä käytetään kaksivaiheista testausta. Kehitystyön tuloksena syntyneet muutokset testataan ensin erillisessä kehitysjärjestelmässä. Onnistuneen testauksen jälkeen muutokset viedään tuotantojärjestelmän kanssa identtiseen testijärjestelmään, jossa suoritetaan lopullinen hyväksyntätesti ennen muutosten vientiä tuotantoon.

Kaikki tuotantoon vietävät järjestelmän muutokset dokumentoidaan huolellisesti.

6.5.2 Tietoturvallisuuden hallinta

6.5.2.1 Tietoturvallisuuden ylläpito

Varmentaja noudattaa tietoturvallisuuden hallinnassa Soneran yritysturvallisuusyksikön määrittelemää politiikkaa. Lisäksi Varmentaja noudattaa kaikessa toiminnassaan määrittelemiänsä tietoturvapolitiikkaa, varmennepolitiikkaa ja varmennuskäytäntöä. Toiminnan auditointi on kuvattu kappaleessa 2.8 ”Toiminnan auditointi”.

Varmentajan laatiman liiketoiminnan jatkuvuussuunnitelman ylläpitoon sisältyy liiketoiminnan riskien arviointi sekä toimintamallien luonti mahdollisten riskien varalta. Raportointi poikkeamista ja havaituista tai epäillyistä suojauksen heikkouksista hoidetaan Varmentajan määrittelemien menettelytapojen mukaan.

Varmentaja huolehtii sopimuksin tietoturvan säilymisestä ulkoistettujen toimintojen osalta sekä määriteltyjen politiikkojen ja käytäntöjen noudattamisesta alihankkijoita käytettäessä.

6.5.2.2 Resurssien hallinta

Varmentaja noudattaa käyttämiensä resurssien sekä tuottamansa ja käyttämänsä tiedon suojauksessa laatimansa tietoturvapolitiikan periaatteita.

6.5.2.3 Käyttöpalvelun hallinta

Käyttöpalvelun hallinta perustuu Varmentajan tietoturvapolitiikan toteuttamiseen, Varmentajan laatiman ohjeistuksen noudattamiseen ja alihankkijoiden kanssa tehdyissä sopimuksissa määriteltyjen vastuiden toteuttamiseen sekä tietoturvapolitiikan, ohjeistuksen ja vastuiden edellyttämän toiminnan valvontaan.

6.5.2.4 Järjestelmien pääsynvalvonta

Varmentajan järjestelmien käyttöoikeuksien hallinnassa ja pääsynvalvonnassa noudatetaan tietoturvapolitiikan periaatteita ja Varmentajan määrittelemää käytäntöä. Eri järjestelmien käyttöoikeuksien hallintaa hoitavat Varmentajan erikseen valtuuttamat henkilöt.

6.5.2.5 Salausteknisen laitteen elinkaaren hallinta

Varmentaja on laatinut ohjeen varmenteiden ja sulkulistojen allekirjoitukseen käytettävän salausteknisen laitteen elinkaaren hallintamenettelystä varmennepolitiikoissa määriteltyjen vaatimusten toteuttamiseksi.

TeliaSonera Finland Oyj

6.6 Verkon turvallisuuden hallinta

Varmentajan järjestelmä on erotettu julkisesta verkosta palomuurein. Kriittisimmät järjestelmän osat on täysin erotettu julkisesta verkosta. Käytössä on myös hyökkäyksentunnistusjärjestelmä.

Varmentajan järjestelmän osien välisessä liikenteessä käytetään vahvaa tunnistusta sekä salausta.

7 Varmenteiden ja sulkulistojen (CRL) profiilit

7.1 Varmenteen profiili

Alla on kuvattu Varmentajan myöntämien eri varmennetyyppien sisältämät tiedot. Varmenteessa tiedot on sijoitettu perättäisiin kenttiin. Osa kentistä on sellaisia, että niiden sisällöt ovat samat kaikissa samaan varmennetyyppiin kuuluvissa varmenteissa, osa kentistä sisältää Varmenteen haltijakohtaista yksilöllistä tietoa.

Varmenteen sisältömäärittely eli varmenneprofiili määrittelee varmenteessa käytettävät kentät. Sonera PKI:hin kuuluvien varmenteiden varmenneprofiili noudattaa ITU X.509 –standardissa määriteltyä versio 3:n mukaista profiilia. Varmenteiden profiili noudattaa myös dokumenttia RFC 3280 ”Internet X.509 Public Key Infrastructure Certificate and CRL Profile".

7.1.1 Varmenteen kentät ja niiden sisällöt

7.1.1.1 Varmenteen peruskentät

Varmenteissa käytetään X.509-standardissa määritellyistä varmenteen peruskentistä ainoastaan kaikkia pakollisia kenttiä. Valinnaiset kentät mahdollistaisivat Varmentajan tai Varmenteen haltijan nimen käyttöönoton uudelleen muille. Nimien halutaan kuitenkin säilyvän yksikäsitteisinä.

Alla on lueteltu varmenteissa käytetyt peruskentät:

Versio (Version)
Sarjanumero (Serial number))
Allekirjoitusalgoritmi (Signature algorithm)
Varmenteen myöntäjä (Issuer)
Voimassaoloaika (Validity)
Varmenteen haltija (Subject)
Varmenteen haltijan julkisen avaimen tiedot (Subject public key info)

7.1.1.2 Varmenteen lisäkentät

Varmenteissa käytetään seuraavia X.509 –standardissa määriteltyjä lisäkenttiä:

Varmentajan avaimen tunniste (Authority key identifier)
Varmenteen haltijan avaimen tunniste (Subject key identifier)
Varmennepolitiikat (Certificate policies)
Sulkulistan julkaisupaikka (CRL distribution points)
Avaimen käyttötarkoitus (Key usage)
Avaimen käyttötarkoituksen laajennus (Extended key usage)
Perusrajoitukset (Basic constraints)
Varmenteen haltijan vaihtoehtoinen nimi (Subject alternative name)

X.509-standardi sallii myös itse määritellyt lisäkentät. Tietyissä varmennetyypeissä käytetään seuraavaa yksityistä lisäkenttää:

Toimikortin sarjanumero (Smartcard serialnumber)

Lisäkenttä määritellään kriittiseksi, kun varmennetta hyödyntävän järjestelmän halutaan hylkäävän varmenteen, mikäli se ei tunnista kriittiseksi määriteltyä lisäkenttää. Yllä mainituista lisäkentistä kriittiseksi on merkitty:

Avaimen käyttötarkoitus (poikkeuksena tietyntyyppisellä toimikortilla oleva varmenne)
Perusrajoitukset (vain Varmentajan varmenteissa)

7.1.1.3 Varmenteen kenttien sisällöt

Alla oleva taulukko sisältää ne varmenteiden kentät, jotka ovat käytössä kaikissa Sonera PKI:hin kuuluvissa varmenneluokissa lukuunottamatta Varmentajan varmenteita.

Kentän nimi	Field name	Kentän kuvaus ja sisältö
Versio	Version	Tässä kentässä ilmoitetaan minkä X.509-standardissa määritellyn version mukainen varmenne on. Sonera PKI:hin kuuluvat varmenteet ovat version 3 mukaisia.
Sarjanumero	Serial number	Varmentaja luo jokaiselle varmenteelle oman sarjanumeron. Tässä kentässä ilmoitettu numero on yksikäsitteinen jokaiselle varmenteelle, joka luodaan Varmentajan järjestelmässä. Ohjelmisto huolehtii automaattisesti sarjanumeron yksikäsitteisyydestä.
Allekirjoitus-algoritmi	Signature algorithm	Allekirjoitusalgoritmi on se matemaattinen säännöstö, jonka mukaisesti Varmentajan ohjelmisto suorittaa varmenteen allekirjoituksen. Yleisesti käytetyille algoritmeille on määritelty tunnisteet. Tässä kentässä ilmoitetaan varmenteen allekirjoituksessa käytetyn algoritmin tunniste. Allekirjoitusta ei voi todentaa, jos käytetty algoritmi ei ole tiedossa. Sonera PKI:hin kuuluvien varmenteiden allekirjoituksessa käytetty algoritmi on sha1RSA.
Varmenteen myöntäjä	Issuer	Tässä kentässä ilmoitetaan Varmenteen myöntäjän nimi. Sama Varmentaja voi myöntää eri luokkiin kuuluvia varmenteita eri Issuer-nimillä. Kunkin varmenneluokan varmenteissa oleva Issuer-nimi on kuvattu asianomaisen varmennepolitiikan kappaleessa 3.1 ”Nimeämiskäytäntö Varmentajan varmenteissa”.
Voimassaolo-aika	Validity	Varmenteen voimassaoloaika on se aikaväli, jolloin Varmentaja takaa ylläpitävänsä tietoa varmenteen tilasta eli siitä, onko varmenne mahdollisesti peruutettu. Tässä kentässä ilmoitetaan päivämäärä ja kellonaika, jolloin varmenne astuu voimaan, sekä päivämäärä ja kellonaika, jonka jälkeen varmenne ei ole enää voimassa. Varmenteeseen voi luottaa sen voimassaoloaikana, jollei varmennetta ole julkaistu sulkulistalla.
Varmenteen haltija	Subject	Tässä kentässä yksilöidään kenen henkilön tai minkä Laitteen hallussa on se yksityinen avain, jota vastaava julkinen avain varmenteessa on. Kenttä sisältää Varmenteen haltijan yksikäsitteisen nimen. Kentän sisältö on kuvattu lyhyesti varmennuskäytännön kappaleessa 3.2 ”Uuden Varmenteen haltijan rekisteröinti” ja tarkemmin kunkin varmennepolitiikan kappaleessa 3.2 ”Uuden Varmenteen haltijan rekisteröinti”.
Varmenteen haltijan julkisen avaimen tiedot	Subject public key info	Tässä kentässä ilmoitetaan se algoritmi, jonka kanssa Varmenteen haltijan julkista avainta käytetään. Sonera PKI:hin kuuluvissa varmenteissa kyseinen algoritmi on RSA. Tässä kentässä annetaan myös itse Varmenteen haltijan julkinen avain.

		Sonera PKI:ssä julkisen avaimen pituus Varmenteen haltijoiden (ei Varmentajan) varmenteissa on 1024 bittiä (lukuun ottamatta kappaleessa 6.2.4 ”Varmenteen haltijan avainten pituudet” mainittua poikkeusta).
Varmentajan avaimen tunniste	Authority key identifier	Tässä kentässä annetaan Varmentajan julkisen avaimen tunniste. Tunnisteen avulla voidaan yksilöidä julkinen avain, joka vastaa varmenteen allekirjoittamiseen käytettyä yksityistä avainta. Sonera PKI:ssä tunnisteen muodostamiseen käytetään SHA-1-tiivistealgoritmia.
Varmenteen haltijan avaimen tunniste	Subject key Identifier	Tässä kentässä annetaan varmenteessa olevan Varmenteen haltijan julkisen avaimen tunniste. Tunnistetta voidaan käyttää löytämään varmenteet, jotka sisältävät tietyn julkisen avaimen. Sonera PKI:ssä tunnisteen muodostamiseen käytetään SHA-1-tiivistealgoritmia.
Varmenne-politiikat	Certificate policies	Tätä kenttää käytetään ilmoittamaan politiikat, joiden mukaisesti varmenne on myönnetty. Politiikka tunnistetaan sille annetun yksilöllisen tunnisteen (Object identifier, OID) avulla. Tunniste on ilmoitettu kunkin varmennepolitiikan kappaleessa 1.2 ”Dokumentin tunnus”.
Sulkulistan julkaisupaikka	CRL distribution points	Tässä kentässä ilmoitetaan mistä sulkulista on noudettavissa. Sonera PKI:hin kuuluvissa varmenteissa tässä kentässä on URI-tyyppinen sulkulistan osoite. Eri varmenneluokkiin liittyvien sulkulistojen tarkat osoitteet on ilmoitettu kappaleessa 4.4.6 ”Sulkulistan tarkistamisvelvollisuus”.

Class 1

Alla oleva taulukko sisältää ne varmenteiden kentät, joita lisäksi käytetään Sonera Class 1 -varmenteissa.

Kentän nimi	**Field name**	**Kentän kuvaus ja sisältö**
Avaimen käyttötarkoitus	Key usage	Varmenteen sisältämän julkisen avaimen käyttötarkoitukset ilmoitetaan tässä kentässä. Varmentaja ei vastaa käyttötarkoitusten vastaisesta käytöstä. Alla on listattu varmenteiden julkisten avainten käyttötarkoitukset. Toimikortille tallennettu varmenne, allekirjoitusavain: NonRepudiation Toimikortille tallennettu varmenne, tunnistus/salausavain: DigitalSignature, KeyEncipherment, DataEncipherment * USB-avaimelle tallennettu varmenne: DigitalSignature, NonRepudiation, KeyEncipherment, DataEncipherment, KeyAgreement * ei käytössä kaikissa varmenteissa
Avaimen käyttö-tarkoituksen laajennus	Extended key usage	Tässä kentässä ilmoitetaan julkisen avaimen muut kuin kentässä ”Key Usage” ilmoitetut sallitut käyttötarkoitukset. Tässä kentässä ilmoitettu käyttötarkoitus saattaa olla yleisesti tunnettu tai tiettyä sovellusta varten itse määritelty.

		Sonera Class 1 –varmenteessa voi olla mainittuna mm. seuraavia käyttötarkoituksia: ClientAuthentication, WindowsLogon, SMIME
Varmenteen haltijan vaihto-ehtoinen nimi	Subject alternative name	Tämän kentän avulla voidaan liittää vaihtoehtoisia tunnistetietoja Varmenteen haltijaan. Sonera Class 1 –varmenteessa voi olla mainittuna mm. seuraavia tunnistetietoja: EmailAddress, WindowsAccountName
Toimikortin sarjanumero	Smartcard serial number	Varmenteen haltijan toimikortin sarjanumero ilmoitetaan tässä kentässä. Sarjanumeroa käytetään liittämään Varmenteen haltija tämän käytössä olevaan salaustekniseen välineeseen. Sarjanumerona käytetään tarkisteella varustettua yksilöllistä numeroa, joka kuuluu Varmentajan toimikorteille varattuun numeroavaruuteen ja joka tallennetaan toimikortille. Kenttää voidaan käyttää hyväksi myös muiden salausteknisten välineiden yhteydessä ilmaisemaan ko. välineen tyyppi. Kenttä on käytössä myös USB-avaimille tallennetuissa varmenteissa, ja sen sisältö on Varmentajan määrittelemä merkkijono.

Class 2

Alla oleva taulukko sisältää ne varmenteiden kentät, joita lisäksi käytetään Sonera Class 2 -varmenteissa.

Kentän nimi	**Field name**	**Kentän kuvaus ja sisältö**
Avaimen käyttötarkoitus	Key usage	Varmenteen sisältämän julkisen avaimen käyttötarkoitukset ilmoitetaan tässä kentässä. Varmentaja ei vastaa käyttötarkoitusten vastaisesta käytöstä. Alla oleva lista sisältää julkisten avainten käyttötarkoitukset, jotka voivat olla mainittuna Sonera Class 2 –varmenteessa. Kaikki listalla olevat käyttötarkoitukset eivät sisälly kaikkiin varmenteisiin, ja joissain Class 2 –varmenteissa käyttötarkoitusta ei ole annettu ollenkaan. DigitalSignature, NonRepudiation, KeyEncipherment, DataEncipherment, KeyAgreement, KeyCertSign, CRLSign
Avaimen käyttö-tarkoituksen laajennus	Extended key usage	Tässä kentässä ilmoitetaan julkisen avaimen muut kuin kentässä ”Key usage” mahdollisesti ilmoitetut sallitut käyttötarkoitukset. Tässä kentässä ilmoitettu käyttötarkoitus saattaa olla yleisesti tunnettu tai tiettyä sovellusta varten itse määritelty. Sonera Class 2 –varmenteessa voi olla mainittuna mm. seuraavia käyttötarkoituksia: CodeSigning, ServerAuthentication
Perusrajoitukset	Basic	Tässä kentässä voidaan ilmoittaa eksplisiittisesti onko kyseessä

	constraints	Varmentajan varmenne (eli Varmenteen haltijana on Varmentaja) vai ei. Joissain Sonera Class 2 –varmenteissa on ilmoitettu että kyseessä ei ole Varmentajan varmenne.
Varmenteen haltijan vaihto-ehtoinen nimi	Subject alternative name	Tämän kentän avulla voidaan liittää vaihtoehtoisia tunnistetietoja Varmenteen haltijaan. Sonera Class 2 –varmenteessa voi olla mainittuna mm. seuraavia tunnistetietoja: EmailAddress, IPAddress
Toimikortin sarjanumero	Smartcard serial number	Kenttää käytetään hyväksi joissain Sonera Class 2 –varmenteissa ilmaisemaan se palvelu tai toiminto, jonka yhteydessä varmennetta käytetään. Näissä tapauksissa kentän sisältönä käytetään Varmentajan määrittelemiä merkkijonoja.

Mobiilivarmenne

Alla oleva taulukko sisältää ne varmenteiden kentät, joita lisäksi käytetään Sonera Mobiilivarmenteissa.

Kentän nimi	Field name	Kentän kuvaus ja sisältö
Avaimen käyttötarkoitus	Key usage	Varmenteen sisältämän julkisen avaimen käyttötarkoitukset ilmoitetaan tässä kentässä. Varmentaja ei vastaa käyttötarkoitusten vastaisesta käytöstä. Alla on listattu varmenteiden julkisten avainten käyttötarkoitukset. DigitalSignature, KeyEncipherment, DataEncipherment
Toimikortin sarjanumero	Smartcard serial number	Varmenteen haltijan Varmenne-SIM -kortin sarjanumero ilmoitetaan tässä kentässä. Sarjanumeroa käytetään liittämään Varmenteen haltija tämän käytössä olevaan salaustekniseen välineeseen. Sarjanumerona käytetään Varmenne-SIM -kortin ICCID-numeroa.

Varmentajan varmenne

Alla oleva taulukko sisältää ne varmenteiden kentät, jotka ovat käytössä Varmentajan varmenteissa Sonera PKI:ssa.

Kentän nimi	Field name	Kentän kuvaus ja sisältö
Versio	Version	Ks. kuvaus yllä olevista taulukoista.
Sarjanumero	Serial number	Ks. kuvaus yllä olevista taulukoista.

Allekirjoitus-algoritmi	Signature algorithm	Ks. kuvaus yllä olevista taulukoista.
Varmenteen myöntäjä	Issuer	Ks. kuvaus yllä olevista taulukoista.
Voimassaolo-aika	Validity	Ks. kuvaus yllä olevista taulukoista.
Varmenteen haltija	Subject	Tässä kentässä yksilöidään Varmentaja, jonka hallussa yksityinen avain on. Kentän sisältö on identtinen kentän ”Varmenteen myöntäjä” sisällön kanssa, ja se on kuvattu kunkin varmennepolitiikan kappaleessa 3.1 ”Nimeämiskäytäntö Varmentajan varmenteissa”.
Varmenteen haltijan julkisen avaimen tiedot	Subject public key info	Ks. kuvaus yllä olevista taulukoista. Sonera PKI:ssä Varmentajan varmenteissa julkisen avaimen pituus on 2048 bittiä.
Varmenteen haltijan avaimen tunniste	Subject key identifier	Ks. kuvaus yllä olevista taulukoista.
Avaimen käyttötarkoitus	Key usage	Sonera PKI:ssa Varmentajan julkisen avaimen käyttötarkoitukset ovat: KeyCertSign, CRLSign
Perusrajoitukset	Basic constraints	Tässä kentässä ilmoitetaan, että kyseessä on Varmentajan varmenne eli Varmenteen haltijana on Varmentaja.

7.2 Sulkulistan profiili

Alla on kuvattu sulkulistan sisältämät tiedot. Sulkulistalla ilmoitetaan mitkä niistä varmenteista, joiden voimassaoloaika ei ole vielä päättynyt, on peruutettu.

Sulkulistat ovat ITU X.509 –standardissa määritellyn versio 2:n mukaisia. Ne noudattavat myös dokumenttia RFC 3280.

7.2.1 Sulkulistan peruskentät

Sulkulistoissa käytetään kaikkia X.509-standardissa määriteltyjä sulkulistan peruskenttiä, sekä pakollisia että valinnaisia.

Alla on lueteltu sulkulistoissa käytetyt peruskentät:

Versio (Version)
Allekirjoitusalgoritmi (Signature algorithm)
Sulkulistan julkaisija (Issuer)
Sulkulistan julkaisuaika (This update)

Seuraavan sulkulistan julkaisuaika (Next update)
Peruutetut varmenteet (Revoked certificates)

7.2.2 Sulkulistan lisäkentät

Sulkulistoissa käytetään seuraavia X.509 –standardissa määriteltyjä lisäkenttiä:

Syy varmenteen peruuttamiseen (Reason code)
- peruutettuun varmenteeseen liittyvä lisäkenttä
Sulkulistan allekirjoitusavaimen tunniste (Authority key identifier)
Sulkulistan järjestysnumero (CRL number)

Lisäkenttä määritellään kriittiseksi, kun halutaan, että varmenteen voimassaoloa sulkulistalta tarkistava järjestelmä tulkitsee tarkistuksen epäonnistuneeksi, mikäli se ei tiedä kuinka lisäkenttä tulisi käsitellä. Mitään edellä mainituista lisäkentistä ei ole määritelty kriittiseksi Sonera PKI:ssä.

Yksityisiä itse määriteltäviä lisäkenttiä ei käytetä.

7.2.3 Sulkulistan kenttien sisällöt

Kentän nimi	**Field name**	**Kentän kuvaus ja sisältö**
Versio	Version	Tässä kentässä ilmoitetaan minkä X.509-standardissa määritellyn version mukainen sulkulista on. Sonera PKI:ssä sulkulistat ovat version 2 mukaisia.
Allekirjoitus-algoritmi	Signature algorithm	Sulkulistojen allekirjoitukseen käytetään samaa algoritmia kuin varmenteiden allekirjoitukseen. Algoritmi on sha1RSA.
Sulkulistan julkaisija	Issuer	Tässä kentässä ilmoitetaan Sulkulistan julkaisijan nimi. Sonera PKI:ssä nimi on aina sama kuin listalla olevien varmenteiden myöntäjän (Varmentajan) nimi.
Sulkulistan julkaisuaika	This update	Päivämäärä ja kellonaika, jolloin sulkulista on julkaistu.
Seuraavan sulkulistan julkaisuaika	Next update	Päivämäärä ja kellonaika, johon mennessä seuraava sulkulista julkaistaan. Seuraava sulkulista voidaan julkaista milloin tahansa edellisen sulkulistan julkaisun jälkeen, kuitenkin ennen siinä ilmoitettua seuraavan sulkulistan julkaisuaikaa. Sonera PKI:ssa ”This update” -ajan ja ”Next update” -ajan välinen erotus on maksimissaan 48 tuntia.
Peruutetut varmenteet	Revoked certificates	Tässä kentässä ilmoitetaan peruutettujen varmenteiden sarjanumerot sekä jokaisen peruutetun varmenteen osalta erikseen aika jolloin varmenne peruutettiin sekä peruuttamisen syy. Peruuttamisen syy voi olla jokin seuraavista: KeyCompromise, CACompromise*, AffiliationChanged, Superseded, CessationOfOperation, CertificateHold

		* vain Varmentajan varmenteen peruuttamisessa
Sulkulistan allekirjoitus-avaimen tunniste	Authority key identifier	Tässä kentässä annetaan sulkulistan julkaisijan julkisen avaimen tunniste. Tunnisteen avulla voidaan yksilöidä julkinen avain, joka vastaa sulkulistan allekirjoittamiseen käytettyä yksityistä avainta. Sonera PKI:ssa tunnisteen muodostamiseen käytetään SHA-1-tiivistealgoritmia.
Sulkulistan järjestysnumero	CRL number	Järjestysnumero ilmaisee kuinka mones Varmentajan julkaisema sulkulista on kyseessä. Numerointi alkaa 1:stä ja se kasvaa aina yhdellä seuraavaan sulkulistaan. Käyttäjä pystyy numeron perusteella päättelemään korvaako jokin tietty sulkulista jonkin toisen sulkulistan.

8 Varmennuskäytännön hallinnointi

Aina kun jotain kohtaa varmennepolitiikassa muutetaan, muutoksen vaikutukset varmennuskäytäntöön arvioidaan. Samoin toimitaan, kun muutetulle varmennepolitiikalle myönnetään uusi objektitunniste (OID). Varmentajan Varmennepolitiikkayksikkö vastaa arvioinnin käynnistämisestä. Dokumentin muuttamiseen voi olla myös muita varmennepolitiikan muutoksista riippumattomia syitä.

8.1 Muutoskäytännöt

8.1.1 Muutokset, jotka eivät vaadi ilmoitusta

Tähän dokumenttiin voidaan tehdä oikeinkirjoitukseen ja ulkoasuun liittyviä korjauksia, sekä muutoksia yhteystietoihin ilman ilmoitusta dokumentin käyttäjille. Dokumentista voidaan myös julkaista käännöksiä eri kielillä ilman erillistä ilmoitusta.

8.1.2 Muutokset, jotka vaativat ilmoituksen

Seuraavat muutokset vaativat ilmoituksen:

- Osapuolten välisiin sopimusehtoihin vaikuttavista muutoksista ilmoitetaan kyseisten sopimusehtojen mukaisesti.
- Mitä tahansa varmennuskäytännön kohtaa voidaan muuttaa ilmoittamalla muutoksesta 15 päivää ennen muutoksen voimaanastumista.

Kaikki ilmoitusta vaativat ehdotetut muutokset julkaistaan osoitteessa http://support.partnergate.sonera.com/

Sopimusehtoihin vaikuttavista muutoksista ilmoitetaan kirjallisesti sopimuksen allekirjoittajan yhteystiedoissa mainittuun osoitteeseen.

8.2 Varmennuskäytännön julkaiseminen

Kopio tästä varmennuskäytännöstä on saatavilla sähköisessä muodossa internetistä osoitteesta http://support.partnergate.sonera.com/

8.3 Varmennuskäytännön hyväksymismenettely

Varmennuskäytäntö ja kaikki siihen tehtävät muutokset julkaistaan Varmentajan Varmennepolitiikkayksikön hyväksynnän jälkeen.

Viiteluettelo

[ISO/IEC 9594-8; ITU-T X.509]	Information Technology – Open Systems Interconnection – The Directory: Authentication Framework. Also published as ITU-T Rec. X.509: Public key and attribute certificates frameworks
[RFC 2527]	IETF:n dokumentti: Internet X.509 Public Key Infrastructure – Certificate Policy and Certification Practices Framework
[SAK Laki]	Laki sähköisistä allekirjoituksista (tullut voimaan 1.2.2003)
[PKIX Roadmap]	IETF:n dokumentti: Internet X.509 Public Key Infrastructure: Roadmap
[ETSI TS 101 456 v1.2.1]	ETSI Technical Standard: Policy Requirements for certification authorities issuing qualified certificates
[RFC 3280]	IETF:n dokumentti: Internet X.509 Public Key Infrastructure – Certificate and Certificate Revocation List (CRL) Profile